National Library of Canada
Canadian Theses Service
Ottawa, Canada
K1A 0N4

Bibliothèque nationale du Canada
Service des thèses canadiennes

NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

NL-339 (r. 88/04) c

Canada

THE UNIVERSITY OF ALBERTA

# THE EFFECT OF INFORMATIONAL TECHNOLOGY ON CIVIL LIBERTIES

BY

MICHAEL BURNETT

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES AND RESEARCH IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF LAWS.

FACULTY OF LAW

EDMONTON, ALBERTA

(SPRING, 1990)

National Library of Canada
Canadian Theses Service

Bibliothèque nationale du Canada
Service des thèses canadiennes

Ottawa, Canada
K1A 0N4

## NOTICE

The quality of this microform is heavily dependent upon the quality of the original thesis submitted for microfilming. Every effort has been made to ensure the highest quality of reproduction possible.

If pages are missing, contact the university which granted the degree.

Some pages may have indistinct print especially if the original pages were typed with a poor typewriter ribbon or if the university sent us an inferior photocopy.

Reproduction in full or in part of this microform is governed by the Canadian Copyright Act, R.S.C. 1970, c. C-30, and subsequent amendments.

## AVIS

La qualité de cette microforme dépend grandement de la qualité de la thèse soumise au microfilmage. Nous avons tout fait pour assurer une qualité supérieure de reproduction.

S'il manque des pages, veuillez communiquer avec l'université qui a conféré le grade.

La qualité d'impression de certaines pages peut laisser à désirer, surtout si les pages originales ont été dactylographiées à l'aide d'un ruban usé ou si l'université nous a fait parvenir une photocopie de qualité inférieure.

La reproduction, même partielle, de cette microforme est soumise à la Loi canadienne sur le droit d'auteur, SRC 1970, c. C-30, et ses amendements subséquents.

ISBN 0-315-60256-2

NL-339 (r. 88/04) c

Canada

UNIVERSITY OF ALBERTA

RELEASE FORM

NAME OF AUTHOR: MICHAEL BURNETT

TITLE OF THESIS: THE EFFECT OF INFORMATIONAL TECHNOLOGY ON CIVIL LIBERTIES

DEGREE: MASTER OF LAWS

YEAR THIS DEGREE GRANTED: 1990

PERMISSION IS HEREBY GRANTED TO THE UNIVERSITY OF ALBERTA LIBRARY TO REPRODUCE SINGLE COPIES OF THIS THESIS AND TO LEND OR SELL SUCH COPIES FOR PRIVACY, SCHOLARLY OR SCIENTIFIC RESEARCH PURPOSES ONLY.

THE AUTHOR RESERVES OTHER PUBLICATION RIGHTS, AND NEITHER THE THESIS NOR EXTENSIVE EXTRACTS FROM IT MAY BE PRINTED OR OTHERWISE REPRODUCED WITHOUT THE AUTHOR'S WRITTEN PERMISSION.

M. R. Burnett

11 Cudmore Avenue
Toorak Gardens
South Australia
Australia 5065

DATE: 19-4-90

THE UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled THE EFFECT OF INFORMATIONAL TECHNOLOGY ON CIVIL LIBERTIES submitted by MICHAEL BURNETT in partial fulfilment of the requirements for the degree of Master of Laws.

Gerald L. Gall
Professor G. Gall

Robert A. Franson
Professor R. Franson

Allan Tupper
Professor A. Tupper

DATE: Apr. 17, 1990.

# ABSTRACT

This thesis examines the way in which the utilization of informational technology by government institutions in Canada has affected civil liberties.

The thesis commences with an overview of the informational process. It details the threats posed to civil liberties at each stage of the informational process. It then considers specific issues pertaining to the use of information in Canadian society, including the social insurance number.

The thesis then proceeds to examine the response of Canadian law to these threats to civil liberties. It establishes that the common law is unable to respond effectively to this threat (whether through the tort of privacy or through other torts such as breach of confidence, negligence and defamation.) The thesis then considers the responses by the federal and provincial legislatures to advances in informational technology. Finally, it considers the impact of the Canadian Charter of Rights and Freedoms on the informational process: and in particular, sections 7, 8 and 2(b) of the Charter.

The thesis draws the conclusion that the existing law in Canada is inadequate to protect civil liberties from advances in informational technology. The law is unable to instill in the individual a belief in the fair handling of information by government institutions. Without this belief, the erosion of civil liberties is inevitable.

## TABLE OF CONTENTS

Page

**Chapter I** **Introduction** . . . . . . . . . . . . . . . . . . 1

**Chapter II** **The Impact of Advances in Informational Technology on Civil Liberties** . . . . . . . 10

Part 1 Introduction . . . . . . . . . . . . . . . . . . . 10

Part 2 Overview of the Informational Process. . . 11
(1) Acquisition and Storage of Information . . . . . . . . . . . . . . 15
(2) Analysis and Use of Information . . . 18
(3) Transmission of Information . . . . .

Part 3 The Effect of Informational Technology on the Relationship between Individuals and Government Institutions. . . . . . . . . 20

Part 4 Specific Concerns Relating to the Use of Informational Technology in Canada . . . . 26
(1) Social Insurance Number . . . . . . . . 27
(2) Dissemination Between Government Institutions and the Private Sector . 29
(3) Law Enforcement Agencies. . . . . . . . 30

Part 5 Conclusion . . . . . . . . . . . . . . . . . . 35

**Chapter III** **Common Law Protection of Civil Liberties From Advances in Informational Technology**. 44

Part 1 Introduction . . . . . . . . . . . . . . . . . . 44

Part 2 Tort of Privacy at Common Law. . . . . . . . 45

Part 3 Regulation of the Informational Process by Common Law Torts. . . . . . . . . . . . . 53
(1) Introduction. . . . . . . . . . . . . . . 53
(2) Defamation. . . . . . . . . . . . . . . . 53
(3) Breach of Confidence. . . . . . . . . . 60
(4) Negligence. . . . . . . . . . . . . . . . 67
(5) Trespass. . . . . . . . . . . . . . . . . 70
(6) Nuisance. . . . . . . . . . . . . . . . . 71
(7) Conclusion. . . . . . . . . . . . . . . . 74

**Chapter IV** **Federal Legislation**. . . . . . . . . . . . . . 87

Part 1 Introduction . . . . . . . . . . . . . . . . . . 87

Part 2 Privacy Act. . . . . . . . . . . . . . . . . . 88
(1) Application of the Act. . . . . . . . . 88
(2) Scope of the Act. . . . . . . . . . . . 89
(a) Right of Access in the

Privacy Act. . . . . . . . . . . . 90
(i) Exempt Databanks. . . . . 92
(ii) Exclusions from the Operation of the Act. . . 96
(iii) Exceptions to the Right of Access . . . . . 99
(iv) Summary of Effects of Exemptions to Right of Access . . . . . . . . 104
(b) Standards in Handling Personal Information . . . . . . 106
(i) The Enacted Standards . . 106
(ii) Enforcement of Sections 4-8 of the Privacy Act. . 112
(c) Indexing of Information Banks of Federal Government Institutions . . . . . . . . . . 115
(d) Right of Privacy Under the Privacy Act. . . . . . . . . . . 116
(3) Conclusion. . . . . . . . . . . . . . . 123

Part 3 Access to Information Act. . . . . . . . . 123

Part 4 The Criminal Code. . . . . . . . . . . . . . 126
(1) Introduction. . . . . . . . . . . . . . 126
(2) Operation of the Act. . . . . . . . . . 129
(3) Judicial Warrant System . . . . . . . . 131
(a) Introduction . . . . . . . . . . 131
(b) Authorization of Warrants. . . . 133
(4) Safeguards. . . . . . . . . . . . . . . 136
(5) Enforcement Provisions. . . . . . . . . 140
(6) Charter . . . . . . . . . . . . . . . . 143
(7) Conclusion. . . . . . . . . . . . . . . 144

**Chapter V Provincial Legislation** . . . . . . . . . . 161

Part 1 Introduction . . . . . . . . . . . . . . . . 161

Part 2 The Privacy Acts of British Columbia, Manitoba, Saskatchewan and Newfoundland. . 162
(1) Privacy Under the Acts. . . . . . . . . 162
(2) Exemptions Under the Acts . . . . . . . 165
(3) Conclusion. . . . . . . . . . . . . . . 168

Part 3 Provincial Freedom of Information Acts . . 169

Part 4 The Ombudsman Act. . . . . . . . . . . . . . 172
(1) Jurisdication of the Ombudsman. . . . . 172
(2) Exclusions of Jurisdiction. . . . . . . 174
(3) Enforcement Procedures. . . . . . . . . 177
(4) Conclusion. . . . . . . . . . . . . . . 177

**Chapter VI Protection From Advances in Informational Technology Under the Canadian Charter of**

**Rights and Freedoms** . . . . . . . . . . . . 185

Part 1 Introduction . . . . . . . . . . . . . . . . . . 185

Part 2 Section 7. . . . . . . . . . . . . . . . . . . . 188
- (1) Introduction. . . . . . . . . . . . . . . 188
- (2) Judicial Interpretation of Section 7 to Date . . . . . . . . . . 189
- (3) Protection Afforded Against Informational Technology by the Current Definition of Section 7 . . . . 195
- (4) A Right of Privacy Under Section 7. . 207
- (5) Conclusion. . . . . . . . . . . . . . . . 218

Part 3 Section 8. . . . . . . . . . . . . . . . . . . . 219
- (1) Introduction. . . . . . . . . . . . . . . 219
- (2) What Constitutes a Search or Seizure. 221
  - (a) Electronic Surveillance. . . . . 222
  - (b) Administrative Searches and Seizures . . . . . . . . . . . . . . 224
    - (i) Administrative Demands for Information . . . . . 227
    - (ii) Voluntary Supply of Information. . . . . . 230
- (3) Reasonableness of the Search and Seizure . . . . . . . . . . . . . . . 232
  - (a) Administrative Search and Seizure. . . . . . . . . . . . . . 233
  - (b) Reasonable and Probable Grounds for the Commission of an Offence 238
- (4) Applicability of Section 1 of the Charter . . . . . . . . . . . . . . . . 239
- (5) Section 8 and a Right of Privacy. . . 241
- (6) Conclusion. . . . . . . . . . . . . . . . 243

Part 4 Section 2(b) . . . . . . . . . . . . . . . . . 244
- (1) Introduction. . . . . . . . . . . . . . . 244
- (2) Informational Practices Inhibiting Freedom of Expression . . . . . . . . . 246
- (3) Access to Information and Section 2(b). . . . . . . . . . . . . . 252
- (4) Conclusion. . . . . . . . . . . . . . . . 257

**Chapter VII International Protection** . . . . . . . . . 280

Part 1 Universal Declaration of Human Rights. . . 281

Part 2 International Covenant on Civil and Political Rights . . . . . . . . . . . . . . 286

Part 3 Conclusion . . . . . . . . . . . . . . . . . . 288

**Chapter VIII Conclusion** . . . . . . . . . . . . . . . . . 296

# CHAPTER I - INTRODUCTION

Technology has provided government institutions with the means to acquire, hold and disseminate far more information than has ever before been possible.[1] As a consequence, there has been an increase in the use and circulation of information within society.[2] Government institutions now possess and rely on more information in performing their statutory functions and in making administrative decisions. The benefits are immediate and visible:[3] the information is used by government institutions to fulfill their objective of ensuring the health, welfare and safety of citizens in society;[4] to better monitor government programmes, to allocate resources equitably and without discrimination; and to improve government planning.[5] In short, government institutions are able to provide a better and more efficient service to citizens.[6]

On the other hand, the advancement in informational technology has had a profound effect on the civil liberties of individuals. The direct effect on civil liberties has been that government institutions have been able to intrude further into the lives of individuals to acquire personal information.[7] The lives of individuals may be traced from birth.[8] Government institutions thus have the power to use this information for purposes not sanctioned by the individual and of which the individual is not aware.[9]

However, the threat to civil liberties goes further. Access to informational technology has altered the nature of the relationship between individuals and government institutions. Substantial institutions having the capacity to utilize information, have enhanced their power.[10] This increased institutional power has prevented individuals from asserting their various liberties. As Duncanson and Kerruish state:

> Civil liberty, to be real and effective here, must operate with an adequate concept of the individual human agent and of power in all its dimensions. Because the individual is a socially constructed centre of expectations, desires and claims, some attention must be paid to the means by which power affects the process of construction not only as a visible restraint but also as a less visible foreclosure of possibilities, encouraging passivity and inducing a feeling of helplessness[11]

Informational technology, as we shall see in Chapter II, has induced such passivity and feelings of helplessness in the individual.

The challenge facing the law is to reverse this erosion of civil liberties caused by the increased use of informational technology by government institutions. Because the threat contains not only an objective aspect (the intrusion into the individual's life), but also a subjective aspect (the passivity and helplessness induced in individuals which prevents them from exercising their liberties), the law must go further than merely regulating the informational process and attempt to restore the confidence of the individual in the fair handling of information by government institutions.[12] It is only if the latter is achieved, that the individual will be able to assert his liberties.

Some commentators have suggested that this restoration can be accomplished only by radically restructuring society, so that social values are given greater emphasis.[13] In this paper we do not propose to consider such fundamental solutions, but rather intend to analyze the existing legal framework in terms of its protection of civil liberties.

As this paper will show, the law in Canada has been slow to respond to the advances in informational technology and the consequential threats to civil liberties. The existing law has only to a limited extent recognized new rights, giving the individual some control over personal information or permitting access to information held by government institutions.[14] These rights are usually collectively referred to as the individual's rights to secure informational privacy.[15] Informational privacy is itself one aspect of the more general right of privacy, which seeks to secure individual autonomy in all spheres of life.[16]

There is no law in Canada which provides a comprehensive response to all of the issues raised by advances in informational technology.[17] We must therefore examine the various laws which may apply to particular aspects of the informational process. These sources of law include the common law and The Canadian Charter of Rights and Freedoms,[18] the most likely source for protection of civil liberties. Various federal and provincial statutes are also relevant. Federally, the most important legislation is the Privacy Act,[19] the Access to Information Act[20] and Part VI of the Criminal Code embodying the Protection of Privacy Act.[21] At the provincial level, Manitoba, Saskatchewan, British Columbia and Newfoundland have enacted Privacy Acts[22] which provide for a statutory tort of privacy. Some provinces have enacted Freedom of Information Acts.[22a] Most provinces have also enacted Ombudsman Acts,[23] which provide some means by which the practices of government institutions may be investigated.

The dilemma facing the law is how to protect the individual's civil liberties on the one hand, and yet allow government institutions to utilize the benefits of technology on the other.[24] The question is:

> where the lines are drawn which on the one hand maintain the rights of individuals, whilst on the other hand, does not interfere with the necessary and legitimate functions of government.[25]

The conclusion drawn by this paper is that the present law in Canada does not satisfactorily achieve this balance. In particular, the laws to which reference has been made do not adequately protect civil liberties from the advances that have been made in informational technology. Without significant reform, the law in Canada is incapable of instilling in the individual a belief in the fair handling of information by government institutions.

The proof of this thesis will involve five distinct stages:

(i) An outline of the advances in informational technology and identification of the ways in which its use by government institutions has eroded civil liberties;

(ii) An examination of the impact of the common law on the informational process and the protection that the common law affords to civil liberties;

(iii) An analysis of the adequacy of the response of the federal and provincial legislatives to advances in informational technology;

(iv) An analysis of the degree to which the Charter of Rights and Freedoms recognizes the rights of informational privacy and the effectiveness of these rights in protecting civil liberties;

(v) An examination of the use which may be made of international law to overcome any restrictive interpretation of the Charter.

## FOOTNOTES - CHAPTER I

1. Westin "Some Forecasts Based on U.S. Experience" in Rowe (ed) *Privacy Computers and You* (1972), 53; Organization for Economic and Cultural Development (O.E.C.D.) "*Digital Information and the Privacy Problem*", Informatic Studies, Vol. 2, 9 (1971); Rankin "Privacy and Technology: A Canadian Perspective" (1984) 22 *Alta. L.R.* 323, 329.

2. Hammond "Misappropriation of Commercial Information" (1986) 64 *Can B.R.* 342, 347.

3. Flaherty "Protecting Privacy in Police Information Systems: Data Protection in the Canadian Police Information Centre" (1986) 36 *U of Toronto L.J.* 116, 157.

4. This being one of the main objectives of government institutions; see Shattuck *Rights of Privacy* (1977) 51.

5. Miller "Computers, Databanks and Individual Privacy: An Overvivew" in Staff of Columbian Human Rights L.R. (ed) *Surveillance Dataveillance and Personal Freedoms Symposium* (1973), 11.

6. Niblett "Computers and Privacy" in Rowe (ed), supra n1 at 17; Government institutions are under pressure to provide better and more responsive services, see Smith "Aspects of the Accountability Problem" in Smith and Hague *The Dilemma of Accountability* (1971), 27.

7. Simons *Privacy in the Computer Age* (1982), 16 citing evidence from Kling's "*Social Analysis of Computers*" (1982) which found that automated record keeping systems held more personally sensitive information about individuals than manual systems.

8. Miller, supra n5 at 11; Benn "Technology and Society" in Rowe (ed); supra n1 at 14.

9. Ryan "Privacy, Orthodoxy and Democracy" (1973) 51 *Can B.R.* 86, 86.

10. Hammond, supra n2 at 347. Westin, supra n1 at 54, refers to the historic libertarian balance of power between the record-keepers and individuals being altered.

11. Duncanson and Kerruish "The Reclamation of Civil Liberty" (1986) 6 _Windsor Yearbook of Access to Justice_ 3, 5.

12. Selmer "Standards for Informational Handling and Control Procedures" in O.E.C.D. _Policy Issues in Data Protection and Privacy_ (1974) Vol 10, Information Studies, 67.

13. eg. Rule McAdam Stearns and Uglow "_The Politics of Privacy_" 1980 153 ff, argue for a looser, more private world.

14. Burkert "Institutions of Data Protection - An Attempt at a Functional Explanation of European National Data Protection Laws" (1981) 3 _Computer L.J._ 167; 170.

15. Chalton & Gaskill (ed) _Encyclopaedia of Data Protection_ (1988), 1002.

16. Flaherty, supra n3 at 118. Sobel (ed) 4 _War on Privacy_ 2 Ryan "Privacy, Orthodoxy and Democracy" (1973) 51 _Can B.R._ 84, 85.

17. Cohen "Invasion of Privacy: Police and Electronic Surveillance in Canada" (1982) 27 _McGill L.J._, 619, 667.

18. Canadian Charter of Rights and Freedoms, as Enacted in Canada Act 1982 (U.K.) c11.

19. Privacy Act, 1982, S.C., 1980-81-82-83, c111.

20. S.C. 1980-81-82-83, c111.

21. R.S.C. 1985, cC-46; For the Protection of Privacy Act, see S.C. 1973-4, c50.

22. Privacy Act, R.S.B.C. 1979, c366; The Privacy Act, R.S.M. 1987, cP125; The Privacy Act, R.S.S. 1978, cP24; The Privacy Act, S.Nfld. 1981, c6.

22a. Infra at p162.

23. Infra at p169.

24. Burkert, supra n14 at 170. Gotlieb "Some Social and Legal Implications of New Technology: The Impact of Communications and Computers" (1973) 51 Can B.R. 244, 246.

25. Sobels, supra n16 at 5. Westin "Privacy and Freedom" (1967) refers to this as the state of political civility where this is enough privacy to nourish individual creativity and group expression, enough publicity of government affairs to let the public know the facts necessary to form a judgment in political matters; and a small area of secrecy for government to preserve the integrity of certain secret information and the privacy of the policy making process.

# CHAPTER II - THE IMPACT OF ADVANCES IN INFORMATIONAL TECHNOLOGY ON CIVIL LIBERTIES

## PART 1. INTRODUCTION

The first stage in the proof of our thesis involves an identification of how informational technology threatens civil liberties. Against this background, the effectiveness of the existing law in providing protection to civil liberties can be judged. In particular, we can then examine whether or not the existing law is sufficient to instill confidence in the individual in the fair handling of information. It is not intended here to indulge in a technical exposé of the latest technological developments.[1] Rather, the purpose in this section is three-fold:

(i) To provide a general overview of the informational process, and to identify the areas where civil liberties are at risk from advances in technology;

(ii) To consider the fundamental changes these advances in informational technology have effected on the relationship between individuals and institutions, and how the ensuing imbalance of power has prevented individuals from attaining the state necessary to exercise their civil liberties;

(iii) To examine specific areas where the use of informational technology in Canada has threatened civil liberties.

## PART 2. OVERVIEW OF THE INFORMATIONAL PROCESS

The information process can be conveniently divided into three stages:

(i) The acquisition and storage of data;

(ii) The analysis and use of data;

(iii) The transmission of data.

Informational technology is the application of computer based techniques to each of the above stages of the informational process.[1a] It has increased the capacity, speed and efficiency of each stage.[2]

### (1) Acquisition and Storage of Information

Informational technology has given government institutions the ability to gather personal information about an individual from a number of new sources.

In the case of direct physical surveillance, government institutions are no longer restricted by the need to trespass on the individual's property to obtain information.[3] For example, the parabolic microphone is now capable of recording conversations from distances over hundreds of metres, without requiring the implanting of a microphone in the vicinity of the conversation.[4] Visual observation has also advanced. Photographs can now be taken by infra red technology, which not only do not require any trespass, but can pass through certain solid structures.[5] Satellite photography is even more indetectable and comprehensive.[6] In the area of simple observation of an individual, the telescopic lens also avoids the need for any trespass.[7]

Even where some form of trespass is required, micro-miniaturization of such devices has made it unlikely that the surveillance will be detected.[8] This has relevance in the areas of listening devices and electronic tracking devices often employed by law enforcement agencies.[9] The tracking device need not be electronic. Fluorescent powders have been developed which are only visible when illuminated by ultra-violet light.[10]

Informational technology has also provided government institutions with the means to share information with each other. All that is required is that on entry into a databank, information is codified in a way compatible with the records of another databank.[11] The use of computers has ensured this compatibility.[12] As a consequence of this linkage of databanks, an institution is able to acquire information about an individual with whom it has no direct relationship. The ease of circulation has thus given government institutions an efficient and quick way to gather information.

Developments in technology have improved the ability of institutions to record actions and transactions.[13] Voluntary information supplied by an individual to a government institution when seeking some service from that institution is able to be recorded. So too is information supplied by an individual to a government institution under threat of penalty for non-disclosure (eg. taxation information).[14]

Information relating to simple everyday occurrences, such as the use of a credit card or cheque, is able to be recorded and placed in a databank. Increasingly, all information will be in a form that allows it to be codified and stored in a databank.[15] It is even now possible to scan a quantity of information to generate a code for input into a databank.[16]

Coinciding with this increased capacity to acquire information has been an increased storage capacity due to miniaturization of product size and greater circuit density.[17] Therefore, vast quantities of information are now able to be conveniently stored. This has altered the type of information capable of being stored. For example, the U.S. Bank Secrecy Act 1971 requires banks to microfilm all cheques and retain them for five years,[18] something that would not have been possible using manual systems.

The increased capacity of government institutions to acquire and store information has impaired the civil liberties of individuals. Direct physical surveillance has resulted, in certain circumstances, in the individual being unable to live, even in his own house, without the fear or actuality of government surveillance. If that individual wishes to be selective in the personal information that he releases to the government, he must modify his behaviour.

Linkage of databanks has caused the individual to lose control over information once it has been supplied to one government institution, even if for a confidential purpose. The individual is therefore unable to meet the government institution which has acquired information about him on equal terms. He starts his dealings from a position of inequality in that the institution has extensive knowledge of his background and has perhaps formed preconceived ideas about him.

The individual has also lost control over information relating to his daily activities and transactions. Again the acquisition of this information by government institutions gives them a greater insight into the personal life of the individual.

In summary, more sensitive information is able to be acquired by government institutions about individuals.[19] The individual is therefore unable to lead his life as he chooses, unless he comes to the decision, at least tacitly, to surrender control of personal information to government institutions.

The task facing the law is to exercise some control over these new modes of acquisition of information and not let governmental practices to go unchecked. The law has not traditionally regulated activities such as the recording of information or the exchange of information between institutions. The inbuilt inefficiency of manual data systems in recording and storing information ensured that these functions did not pose any threat to the liberties of individuals. Further, in the case of direct physical surveillance, the law has only recently regulated forms of surveillance associated with trespass. New technology has produced the means to acquire information without infringing such concepts.

## (2) Analysis and Use of Information

Technological developments have also significantly advanced the second stage of the informational process, namely the analysis and use of data. The physical organization of information has ceased to be a limiting factor[20] and government institutions are able to utilize the vast amounts of information that they have gathered.[21] Technological developments have led to greatly increased speed and capacity to process instructions.[22] This has coincided with a drastic reduction of the cost of performing these functions.[23] In short, government institutions are able to retrieve any piece of information held in a databank quickly and efficiently.[24]

The retrieval function is not merely limited to a mechanical analysis of the information stored in a databank. Rather, it has the capacity, using associational and correlational techniques, to generate new forms of information.[25] It does this by its ability to reorganize large quantities of information, (i.e. with each discrete item of information being harmless) to reveal an unknown fact or pattern which may be harmful to the individual.[26] For example, the fact that an individual stayed at a particular hotel on a given night is an innocent item of information by itself, but further information concerning where that person stayed over a period of a week, may reveal some clandestine pattern.[27] The benefit of associational techniques to law enforcement agencies is obvious.

However, such techniques bring a number of consequences. First, it is likely that they will lead to increased demands for information, as associational techniques require sufficient information to establish a particular pattern. Secondly, a deeper insight is gained into an individual's personal life by these associational techniques.[28] Thirdly, there is the danger that as associational techniques become more advanced, they will be used to predict an individual's behaviour based on background data, rather than on information specifically pertaining to that individual. The United States Internal Revenue Service has already begun to do this. Certain tax returns are analyzed by computer and, if they do not conform to certain "normal" standards, are referred for further investigation.[29] Fourthly, an incomplete and misleading picture may be formed of an individual or his actions because of insufficient or inaccurate data.

An efficient system for the retrieval of information thus assists further intrusion into individuals' lives. The generation of new forms of information has enhanced the capacity of government institutions to make intimate (and possibly wrong) decisions about individuals, without reference to those individuals.[30] The individual thus loses the ability to decide whether or not to surrender personal information to the government institution. Further, the ability of government institutions to categorize individuals is also enhanced. The risk is that individuals may feel compelled to modify their behaviour to avoid an adverse categorization. The result is what Miller calls the age of radical orthodoxy,[31] where individuals attempt at all times to conform to expected standards.

The law has, in the past, generally not interfered with this retrieval process, nor with the use of information by government institutions. The main reason for this position is that the law has regarded institutions as having the right to make their own decisions with the information available. It is not for the law, as long as the discretion is exercised fairly in terms of administrative law principles, to substitute its own decision for that of the government institutions.[32] On a practical level, the lack of access to personal files afforded by a government institution to an individual, will prevent the individual from being aware of the use of his personal information.

**(3) Transmission of Information**

As with other stages of the informational process, the physical ability to transmit information has been greatly improved over recent years.[33] A satellite, for instance, can transmit one billion bytes of memory per minute.[34] A telephone line would take two days to make the same transmission.[35]

In addition to this increased speed and capacity, there are now many more facilities which are capable of receiving this transmission. The telephone, computer terminal and television set can all be used as a terminal to receive and transmit data.[36] The immediate impact of such diversity is decentralized access to databanks. For example, the F.B.I., as long ago as 1972, was said to have five thousand remote access terminals connected to its central files.[37] The linkage of databanks has also facilitated transmission of information. No longer is it necessary for the particular institution to itself possess the information transmitted.

The risk with this increased accessibility to information, is unauthorized and widespread access.[38] There is no need to gain physical access to files to obtain information.[39] Once obtained, the information can be further disseminated without restriction.[40] Any false or misleading information will thus spread at a faster rate to new receivers.[41]

Illegitimate access will also increase, as databanks have a standard access code to individual files. Once a party legitimately obtains access by use of this code to a particular piece of information, that party has the ability to gain access to all other information contained in that file.[42]

The individual is left with little or no control over his personal information.[43] The ability of government institutions with whom he has no direct contact to make personal decisions affecting him is enhanced.

The disclosure of information is the stage of the informational process that has been most regulated by law, probably because it is relatively easy to point to some objective harm befalling an individual because of improper disclosure (eg. as in the case of defamation or breach of confidence). However, advances in technology have obscured the question of what constitutes disclosure. In R v McLaughlin,[44] the accused, without authority, used a computer from the University of Alberta to obtain confidential information. He was charged with theft under section 287(1)(b) of the Criminal Code which included in its definition of theft, use of any telecommunication facility without right.[45] Telecommunication was defined in the Code to include any transmission, emission or reception of signals.[46] The issue therefore was whether the use of a computer to obtain information constituted using a telecommunication facility. On appeal, the court held that it did not, their reasoning being that section 287, as defined, connotes a sender and receiver and the chanelling of information from one to the other.[47] A computer, the court held, did not channel information to an external receiver, rather its operators only made complex calculations and then retrieved those calculations internally.[48]

The law must also deal with the question as to what specific restrictions ought to be placed on the ability of institutions to disclose information. A related question is whether information, gained for one purpose, ought to be permitted to be shared with another institution whose purpose in using that information may be very different.

## PART 3. THE EFFECT OF INFORMATIONAL TECHNOLOGY ON THE RELATIONSHIP BETWEEN INDIVIDUALS AND GOVERNMENT INSTITUTIONS

So far, the direct impact on civil liberties of the advances in informational technology have been considered. These can be summarized as an increase in the degree to which government institutions can intrude into the lives of individuals. The individual loses the ability to act as he wishes unless he chooses to surrender information about his activities to the government. However, in the Introduction to this paper, we foreshadowed a further, indirect effect upon civil liberties. This was a fundamental change in the position of the individual in society,[49] the individual being in a position where he is unable to exercise his other rights and liberties.

The ability to acquire and use vast amounts of information, we have suggested, has lead to an increased value of information as a commodity.[50] Information becomes a crucial factor in the making of decisions and implementation of policies. As Burns says:

> Knowledge (or information) is the key to power in human institutions and the capacity, or will to invade core zones of privacy turns that key.[51]

However, to acquire that information requires the resources of large institutions such as government institutions.[52] They are the possessors of the new tools.

Coinciding with this enhanced power of government institutions has been an actual loss of power to individuals. This has been caused by the anonymity and neutralizing effect of informational technology on the individual, which has led to an inability on the part of the individual to confront government institutions and hold them accountable for their actions.

At a superficial level, this can be seen in holding the computer, rather than an official of a government institution, responsible for a particular decision.[53] A simple case is the incorrect computer invoice.[54] However, the inability to hold government institutions accountable goes further. Informational technology has increased the secrecy of government institutions by:

(i) - Making it more difficult for the average citizen or public interest group to ascertain what information is being kept in automated files;

(ii) By making it more difficult for persons to search through public records (information is often coded in a way incomprehensible to the unskilled reader);[55]

(iii) By creating databanks whose software is geared to efficient operations, rather than disclosure of information.[56]

The resulting secrecy forestalls accountability of government institutions. They are able to manipulate the flow of information to the individual by the selective release of information.[57] Criticism of bureaucratic performance is reduced, as bureaucracies will simply choose not to release adverse information and therefore not subject themselves to outside interference.[58]

This lack of knowledge of the individual of the affairs of government institutions has a more basic legal consequence. The individual is often unable to pursue legal action against government institutions, simply because he is unaware of the facts which may give use to the cause of action. For example, an individual may be unaware of the disclosure by a government institution to a third party of confidential information or a defamatory statement. He may be even unaware that an adverse decision has been made.

In some instances, the individual is deprived of some legal remedies. For example, his name may be placed on a blacklist in a databank.[59] This may constitute a severe penalty (eg. denial of employment, etc.), but there is no legal hearing or even notification of this occurrence.[60]

The disparity of power between government institutions and individuals in relation to the informational process leads to the indirect impairment of the civil liberties of the individual, to which we referred to earlier. At the first stage of the impairment, the individual is prevented from expressing ideas, engaging in criticism or performing certain acts, when he knows that information can be used against him by those in power. As Miller says:

> When a citizen knows his conduct and associations are being put on file and that the information may be used to harass or aggrieve him, he may become concerned about the possible contents of that file and less willing to assert his expressed rights.[61]

This inhibition, or chill factor as it is commonly known, is a recognized psychological reaction, arising from a threatening social situation.[62] Acquisition of information constitutes this threatening situation. Even more threatening would be direct physical surveillance - the very act of surveillance tends to define those activities as "undesirable" or "illegal".[63]

The effect of this chill is that individuals will be dissuaded from carrying out perfectly legitimate activities when they know or perceive that these acts will be observed, recorded and possibly used to their detriment.[64] Thus an individual might not engage in justified public criticism of a particular government institution. He might not associate with certain persons whom he believes are viewed unfavourably by government institutions because of the fear that he would be tainted by such an association.

At the second stage of the impairment of his civil liberties, the individual will not only restrict his actions so as not to provide adverse information to government institutions, but will actually modify his behaviour to obtain a favourable response.[65] Informational technology, with its gathering of information from various sources, has left individuals unaware as to the reasons why a particular decision is made. Accordingly, individuals lose their ability to plan their actions to fit a known set of criteria.[66] As Miller says:

> Many people have come to feel that their success or failure in life may ultimately turn on what other people put in their files and an unknown programmer's ability or inability to evaluate that information.[67]

If, therefore, an individual wishes to affect this evaluation decision, he must alter his behaviour so as to provide data that will more likely produce a desirable result for him. The very act of physical surveillance can also lead to this behaviour modification at a subconscious level. An individual who is aware of surveillance may redefine his activity, which gives rise to that surveillance is illegal.[68]

At its extreme, widespread modification of behaviour, either subconsciously or consciously, will lead to "the age of radical orthodoxy - people holding popular and conformist views".[69] In such a world civil liberties, even if they exist in a legal sense, are illusory because individuals are not in a position to exercise them.

## PART 4. SPECIFIC CONCERNS RELATING TO THE USE OF INFORMATIONAL TECHNOLOGY IN CANADA

Government institutions in Canada have taken advantage of this revolution in informational technology. It has been estimated that "practically one half of Canada's gross national product, and more than one half of the employment of its citizens is related to the production, processing, storage and use of information".[70] Evidence also exists to suggest Canadians are right to be concerned by possible misuse of information by government institutions. As long ago as 1972 the Canadian Task Force on Computers came to the following conclusions:

(i) That more personal information is being collected than most Canadians realize;

(ii) Databanks contain more inaccuracies than is generally realized;

(iii) Citizens do not know what information is being gathered and to what use it is being put.[71]

The Ontario Commission on Freedom of Information and Individual Privacy reached a similar conclusion when it held that more sensitive information on all aspects of our lives is now being kept.[72]

In addition, there are several specific areas in

Canada where government informational practices are justifiably contributing to the concerns of individuals.

### (1) Social Insurance Number

Most prominent of these concerns is anxiety about the Social Insurance Number system. This number was first introduced into Canada in 1936, and since 1965 has been used in tax collection and payment of pensions into the Canadian Pension Plan Act.[73] Section 100(1) of that Act provides that everyone over 18 years of age apply for a Social Insurance Number. Although section 107(i) of that Act provides for the general confidentiality of the information supplied pursuant to this number, there are several exceptions which permit widespread sharing of information between the Departments of National Revenue, Supply and Services, and Unemployment Insurance Commission.[74] In addition, apart from such compulsory uses, the Privacy Commissioner has indicated that the number is also used widely by other government departments, both federally and provincially, and also by private organizations.[75]

The advantage of the Social Insurance Number is its use as a single identifying number.[76] As institutions increase the size of their databanks (which is inevitable given the increased acquisition of information), the accurate identification of one particular individual assumes greater importance to ensure efficient retrieval of information. Linkage of databanks also demands precise identification - "the identifiers and authenticators used by the organizations between which exchanges of records take place must be common to both".[77] There are the resulting advantages of efficiency to the institution and accuracy of records to the individual, especially important in today's highly mobile society.[78]

The primary danger to civil liberties in the use of the Social Insurance Number lies in this ability to facilitate linkage between databanks.[79] The spectre is raised of huge databanks being created through this linkage, and consequent circulation and transmission of intimate details about individuals.

In practice, studies undertaken by the Privacy Commissioner have revealed that there has not been widespread linkage of databanks through use of the Social Insurance Number.[80] However, law enforcement agencies, federally and provincially, have been given routine access to the Social Insurance Number databanks.[81] Furthermore, as stated previously, the Social Insurance Number is being required on an increasing number of forms. This gives rise to three concerns. First, the individual citizen is unaware of the extent of linkage. He only knows that on a myriad of forms he must insert his Social Insurance Number. Therefore, he may perceive that there is widespread linkage of databanks. Such a perception contributes to the individual's disbelief in the fair handling of information by government institutions. Secondly, the potential exists for future linkage of databanks. The information is currently being held in individual databanks with a common identifier (i.e. the Social Insurance Number), hence it would be a simple task to link the databanks at a later stage. It is easy to foresee that concern over future use of information may inhibit, at present, an individual from exercising his rights. Thirdly, there is the danger that once an identifier is in use, it will facilitate uses of that information for purposes other than for which it was originally supplied.[82] The individual loses all control over personal information, which may be shared with institutions with whom he has no direct relationship.

### (2) Dissemination Between the Government Institutions and the Private Sector

The amount of information being disseminated between a government institution and the private sector is also of concern. Various commentators refer to a network linking taxation authorities, police, insurance companies and private investigators.[83] Within this group there is free passing of information.[84] For example, it has been reported that both the federal and provincial governments are clients of the giant American Retail Credit Company - client 156-500 for instance being the Quebec Ministry of Revenue.[85]

The dissemination need not be so formally structured. The Inquiry into the Confidentiality of Health

Records in Ontario revealed that on approximately three hundred occasions, medical information had been supplied to the R.C.M.P. by physicians and hospital employees in Ontario without the prior consent of the patient. The McDonald Commission of Inquiry into Certain Activities of the R.C.M.P. also criticized the relatively routine access afforded to the R.C.M.P. by both government and private sector databanks.[86] Likewise, on request, non-sensitive and, on occasions, sensitive information is often supplied by government institutions to the private sector (eg. to employers through the "old boy network" and "return of favour" system).[87]

Although there is no evidence or suggestion of linkage of databanks between government institutions and private sector, there is obviously widespread transfer of information. The risk to civil liberties lies in this increased circulation of personal information, and also in the perception of government interference in all aspects of our lives.

### (3) Law Enforcement Agencies

The area of government that is most commonly associated with utilization of the advances in informational technology is law enforcement. The Orweillian spectre is raised of police monitoring and intruding into all aspects of individuals' lives. While obviously this scenario has not occurred in Canada, the actions and powers of the law enforcement agencies do, at the very least, suggest a potential risk to civil liberties. This is an area where claims of invasion of civil liberties are especially vulnerable as they conflict with the immediate goal and benefit to society of reducing the crime rate.

Law enforcement agencies, compared with other government departments, have wide powers to acquire information. Under sections 487 and 487.1 of the Criminal Code,[88] they have wide powers of search and seizure and entry onto premises. Under Part VI of the Code they are able to intercept electronic communications subject to obtaining a judicial warrant. Pursuant to section 8(2)(e) of the Privacy Act, information in the databank of a government institution may be disclosed to a law enforcement agency on written request and without the need for a judicial warrant.[89] Information may also be obtained more formally through exchanges of information with the private sector, intervening of witnesses and suspects.

The intelligence forces possess even wider powers than the police to open mail, tap telephones and conduct searches.[90]

The information acquired by law enforcement agencies is stored in a databank known as the Canadian Police Information Centre (C.P.I.C.). C.P.I.C. is described in the Personal Information Index Files as:

> An advanced computerized information storage and retrieval facility designed for the sole use of participating law enforcement agencies. C.P.I.C. acts as a repository of operational police data that is contributed to, and maintained by participating police forces.[91]

Direct access to C.P.I.C. is limited to the R.C.M.P., provincial police forces, city police and some municipal police.[92] However, through the linkage of their own databank, the Automated Criminal Intelligence Information Centre, intelligence forces have indirect access to the files of the C.P.I.C.[92] Once the law enforcement agencies obtain information from C.P.I.C., they may disseminate it to other government agencies responsible for law enforcement (eg. parole officers, probation officers, etc.) on a "need to know" basis, or to other government agencies on approval of the Attorney-General or Solicitor-General.[93]

Obviously, considerable personal information about individuals is stored in the files of C.P.I.C. The Criminal Records File and Motor Vehicle Registration File alone contain 3 million and 4.5 million entries respectively.[94] However, the information contained in these files and the other component files of the C.P.I.C.[95] is at least objective; the Person's File, comprising 1.5 million is of a much more subjective nature. This file contains information on persons believed to have committed a criminal offence, but where there is insufficient information to prosecute that person. The Person's File also contains information on persons known to be dangerous to themselves or others.[96]

The threat to civil liberties posed by the informational practices of law enforcement agencies obviously lies in the vast amounts of personal information that they collect and disseminate.[97] Inaccurate information may be circulated (C.P.I.C. does not guarantee the accuracy of the information).[98] Public fears of a police state in which individual's actions are being constantly monitored will be intensified unless there is adequate supervision of law enforcement surveillance and informational practices to ensure that the interests of the individual are being properly considered.

C.P.I.C. is deficient in establishing statutory standards regulating the databanks or providing for any independent inspection or supervision.[99] At present, C.P.I.C. is supervised by an advisory committee consisting of twenty six Police Officers.[100] Guidelines are drawn up by this supervisory committee, though as indicated previously, these guidelines are of administrative effect only. It is suggested, for the following reasons, that an independent body is required to oversee C.P.I.C. First, there will be a natural bias on the part of the Advisory Committee to identify with police concerns rather than necessarily achieving the proper balance between the goals of law enforcement and the protection of civil liberties.

Secondly, the Committee would be unable to obtain an overall view of the state of privacy of Canadian society and how C.P.I.C. forms a relevant part of that privacy. Rather, it will only consider specific concerns relating to C.P.I.C. Thirdly, there is a need for the reassurance of the public that the operations of the C.P.I.C. are acceptable[101] - a fortiori an independent body seen to be without bias, is best able to provide this reassurance.

It is also clear from the McDonald Commission that the police have not always acted according to their legal power. The Commission found that:

> (i) It has been increasingly apparent that the police have for some considerable time operated illegally (including conducting burglaries and unauthorized wiretapping).
>
> (ii) The R.C.M.P. Security Division took no notice of the difference between legitimate political activities and those activities that would constitute a threat to the national security.[102]

Given, therefore, the wide powers of acquisition of information (including direct physical surveillance), the lack of supervision, and the instances of abuses of these powers, individuals cannot be satisfied that the law enforcement agencies are acting reasonably in the acquisition of information. From this disbelief, we have argued that impairment of civil liberties inevitably follows.

## PART 5. CONCLUSION

The analysis of the effects of the advances in informational technology has, it is submitted, revealed the need to preserve individual liberty in the face of this increased interference by government institutions.[183] We have discussed the ways in which both the general nature of the advances in technology and their specific utilization in Canada will, if improperly controlled and supervised, impair the civil liberties of individuals. What must now be examined is whether existing Canadian law is capable of supplying this control and supervision over the informational practices of government institutions so that individuals may be able to acquire a belief in the fair handling of information by these institutions. We have argued that this belief is necessary if the erosion of civil liberties is to be prevented.

## FOOTNOTES - CHAPTER II

1. For a basic discussion of the operation, in technical terms, of the computer see Mann Computer Technology and the Law in Canada (1987), 6 ff.

1a. Chalton "An Introduction to Informational Technology" 1989 I.L.P. 81, 81.

2. Westin Privacy and Freedom (1967), 137: Organization for Economic Cooperation and Cultural Development (O.E.C.D.) Informatics Studies, Vol. 2, "Digital Information and the Privacy Problems" (1971), 16.

3. For a general discussion of the new devices to acquire information, see Westin, supra n2 at 67 ff.

4. Schafer "Privacy: A Philosophical Overview" in Gibson (ed), "Aspects of Privacy Law in Canada" (1980), 3, quoting Clarke J in Berger v NY 388 US 41, 46-7, (1967); Rankin "Privacy and Technology: A Canadian Perspective" (1984) 22 Alta. L.R. 323, 324.

5. Rankin Ibid 324. Westin supra n2 at 225.

6. Firkellen "A Computer View" in Murray (ed) "Information Processing and the Right to Privacy: A Crossroads Decision for North Americans" (1972), 100.

7. Rankin, supra n4 at 324.

8. Westin, supra n1 at 67; Firkellen, supra n6 at 101.

9. Firkellen Ibid 100. See Fishman "Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo and the Questions Still Unanswered" (1985) 34 Catholic L.R. 277 for discussion of the latest U.S. cases on new forms of electronic tracking devices.

10. Westin, supra n2 at 67.

11. De Weese "Public National Data Planning and Dispersion" in Murray, supra n6, at 32. Rankin, supra n4 at 330.

12. Rankin Ibid.

13. U.S. "Technology and Privacy: The Report of the Privacy Protection Study Commission" (1977), 8.

14. Williams "Invasion of Privacy" (1973) "Alta. L.R. 1, 2.

15. Rankin supra n4 at 324; U.S. "Technology and Privacy: The Report of the Privacy Protection Study Commission" (1977), 20.

16. Rankin Ibid.

17. Janisch and Irwin "Information Technology and Public Policy: Regulatory Implications for Canada" (1982) 20 Osgoode Hall L.J. 610; Rankin supra n4 at 330.

18. Rankin Ibid.

19. Kling "Impact of Computing" in Simons (ed) Privacy in the Computer Age (1982), 108.

20. U.S. "Technology and Privacy: The Report of the Privacy Commissioner" (1977) 21; Rankin supra n4 at 330. DeWeese supra n11 at 31.

21. Shattuck "Rights of Privacy" (1977) xiii, reports that in 1975, the U.S. Government reported that it had collected 92 billion pages of information in 8000 separate systems of files. The list of federal databanks ran to 3100 pages.

22. Janisch and Irwin supra n17 at 613.

23. Ibid.

24. Forget "Assault on Privacy: An Overview" in Murray supra n6 at 4 see retrieval of information as the single most significant aspect of the information process.

25. Niblett "Computers and Privacy" in Rowe (ed) Privacy Computers and You (1972), 21; O.E.C.D. supra n2, at 18.

26. Ibid.

27. O.E.C.D. Ibid.

28. Turin "Privacy and Security in Personal Information (1974), 2.

29. U.S. "Technology and Privacy: The Report of the Privacy Commissioner" (1977) 22.

30. Ryan "Privacy, Orthodoxy and Democracy" (1973) 51 Can B.R. 84, 86.

31. Miller The Assault on Privacy (1971).

32. See eg. Re Ombudsman of Ontario and Health Disciplines Bd (1979) 95 D.L.R. (3rd) 716, 722 where the court makes this point re judicial review.

33. Rankin supra n4 at 330; Westin supra n2.

34. Janisch and Irwin supra n17 at 615.

35. Ibid.

36. Ibid.

37. De Weese supra n11 at 30.

38. Williams supra n14 at 2. Rankin supra n4 at 330.

39. Rankin Ibid; De Weese supra n11 at 30.

40. Williams supra n14 at 2.

41. Ibid.

42. Ross "How the Computer is Changing the Dimensions of the Problem" in Rowe (ed) *Privacy Computers and You* (1972), 27.

43. Williams supra n14 at 2.

44. (1980) 113 D.L.R. (3rd) 386.

45. Criminal Code (Rep & Sub 1974-75-76 c93, Section 23(1), Section 287(1)) "Everyone commits theft who fraudulently, maliciously or without colour of right ... (b) Uses any telecommunications facility or obtains any telecommunications secret."

46. Section 2 defines telecommunication to include "any transmission, emission or reception of signs, signals, writing, images, sounds or intelligence of any nature by radio, visual, electronic or electromagnetic system".

47. (1980) 113 D.L.R. (3rd) 386, 394.

48. Ibid.

49. See Rule, McAdam, Stearns & Uglow "*The Politics of Privacy*" (1980), 72.

50. Hammond "The Misappropriation of Commercial Information in the Computer Age" (1986) 64 *Can*

B.R. 342, 347.

51. Burns "The Law and Privacy: The Canadian Experience" (1976) 54 Can B.R. 161.

52. Hammond supra n50 at 347.

53. De Weese supra n11 at 29.

54. Ibid.

55. See Westin "Technology and Secrecy" in Dorsen (ed) "Our Endangered Rights" 288.

56. Ibid.

57. Rourke "Secrecy and Publicity: Dilemmas of Democracy" (1961) 12.

58. Halperin and Hoffman "Top Secret: National Security and the Right to Know" (1977), 33.

59. Ryan "Assault on Privacy: An Overview" in Murray supra n6 at 19.

60. Ibid.

61. Miller "Computer Data Banks and Individual Privacy: An Overview" in Staff of Columbia H.R.L.R. (ed) "Surveillance, Dataveillance and Personal Freedoms Symposium" (1973), Columbia Human Rights L.R. (special ed), 1, 15.

62. Askin "Surveillance: The Social Science Perspective" in "Surveillance Dataveillance and Personal Freedoms Symposium" supra n61, at 70; Davis "Police Surveillance of Political Dissidents" in "Surveillance, Dataveillance and Personal Freedom Symposium, supra n61 at 126.

63. Ibid 73, Davis supra n62, at 130; Donner

"Electronic Surveillance: The National Security Game" (1978) 2 Civil Liberties Review 15.

65. Ryan supra n59 at 22-23.

66. Miller supra n61 at 18.

67. Ibid.

68. Askin supra n62 at 76.

69. Ryan supra n65 at 22.

70. Rankin supra n4 at 323.

71. Schafer supra n4 at 3 citing Canada, Report of Department of Communications, Department of Justice "Privacy and Computers" (1972), 3.

72. Rankin supra n4 at 332 citing Ontario Commission c27.

73. Rankin Ibid 342. Canada Pension Plan Act S.C. 1965, c51.

74. Sections 107(3), 107(4) Canada Pension Plan Act S.C. 1965, c51.

75. Rankin supra n4 at 342 citing Privacy Commission, Report of the Privacy Commissioner (1981) found that the social insurance number was required in the federal government sphere on a long list of forms ranging from employees' travel claims, to requests for access to personal information, banks and applications for participation in the annual goosehunt. Provincially, it was used on lists of elections or applications for fishing licenses, and in the private sphere it may be required to cash cheques or rent or vacuum cleaners.

76. Canada Report "Privacy and Computers", Department of Communications/Department of Justice (1972) 89;

Rankin supra n6 at 342.

77. U.S. "Technology and Privacy: The Report of the Privacy Commission" (1977), 607.

78. Ibid 608.

79. Ibid.

80. Rankin supra n4 at 343, citing evidence from the report of the Privacy Commissioner.

81. Ibid.

82. Ibid 339.

83. See Miller supra n61 at 20. Ryan supra n65 at 20.

84. Miller Ibid.

85. Ryan supra n83 at 20.

86. Rankin supra n6 at 340.

87. Murray supra n83 at 22.

88. Criminal Code (Rep & Sub 1974-75-76, c93, Section 23(i)).

89. Rankin supra n6 at 340.

90. For a discussion of the powers of the Canadian Security Intelligence Service see Rankin "National Security, Information Accountability and the Canadian Security Intelligence Service" (1986) 36 University of Toronto L.J. 24.

91. Flaherty "Protecting Privacy in Police Information Systems: Data Protection in the Canadian Police

Information Centre" (1986) 36 University of Toronto L.J. 116, 124.

91(a) Ibid.

92. Ibid 130.

93. Ibid 132.

94. Ibid.

95. Ibid. The other files include the Vehicles File, Boat File, Dental Characteristics File, Driving License Records File, Property File.

96. Ibid.

97. For example, there are 1.5 million enquiries of C.P.I.C. per week - see Flaherty supra n91.

98. Ibid.

99. Ibid.

100. Ibid.

101. Ibid.

102. McDonald Commission Vol 2-1.

# CHAPTER III - COMMON LAW PROTECTION OF CIVIL LIBERTIES FROM ADVANCES IN INFORMATIONAL TECHNOLOGY

## PART 1. INTRODUCTION

English law (and Canadian law up until the enactment of the Charter in 1982) did not provide constitutional protection for civil liberties. Civil liberties were, in Blackstone's words, "the very end and scope of the constitution".[1] It was the common law which "regards, asserts and preserves" civil liberties.[2]

The classic doctrine of the British Constitution, formulated by Dicey followed this model. The "absolute legislative sovereignty or despotism of the King in Parliament" was the foundation of Dicey's doctrine.[3] However, also crucial was the role of courts in "interpreting and applying the common law and statute law and in deciding where State power ends and the rights of individuals begin."[4]

The enactment of the Charter does not diminish the importance of the common law in protecting civil liberties, but rather provides for the clear enunciation and elevation of certain rights to the level of constitutionally protected rights which cannot be interfered with by Parliament.[5] Notwithstanding the Charter's enactment, basic protection to civil liberties is still provided by the common law and statute law.[6]

It is therefore necessary to consider how the common law has responded to this threat to civil liberties caused by advances in informational technology. In particular, we must consider whether the common law has provided the individual with any control over information, the exercise of which at some point or another can ensure the end of State power over personal information. As we stated earlier in this paper, it is a right of privacy (including an informational aspect), that provides the individual with this control over information.[7] What must therefore be examined is the extent to which the common law recognizes a right of privacy and the degree of protection such a right affords to civil liberties. Further, if a right of privacy is not recognized at common law, the regulation of the informational process by other common law remedies will be examined.

## PART 2. TORT OF PRIVACY AT COMMON LAW

Fridman succinctly summarizes the status of the tort of privacy in Canada - "at common law it can be said with certainty that there is no right of privacy per se."[8] The reasoning for this position is three-fold.

First, tort law has formulated liability "in terms of reprehensible conduct, rather than of specified interests entitled to protection against harmful invasion."[9] In the informational context, because the law has not assigned any rights to the individual over personal information, it has not been possible to find any wrongdoing and reprehensible conduct on the party invading privacy by the use of information.

The second reason is judicial conservatism.[10] The concept of privacy is very uncertain. The courts are therefore reluctant to introduce a new cause of action when faced with such an uncertain concept.[11] As Dixon J (as he then was) held in Victoria Park Racing Co. v Taylor:[12]

> what acts or omissions result in responsibility and what do not, are matters defined by long established rules of law from which judges ought not wittingly depart and no light is shed upon a given case by large generalisations about them.[12]

Street advances a further reason for this conservation, namely a reluctance by the courts to clash with government by usurping the legislative function of Parliament by the creation of new rights.[13]

The third reason is a policy one. Until recent times there has not been a need to recognize a right of privacy.[14] The inability of manual data systems to acquire, store, collate and disseminate information simply did not pose the threats to civil liberties that we outlined in the preceding Chapter.[15]

However, if the common law is the bulwark of civil liberties, as the earlier commentators suggested, one would expect the common law to evolve with these new threats and declare a new cause of action.

There have been some indication of judicial activism in Canadian Courts in developing a common law right of privacy. The cases usually quoted as evidencing this trend are Krouse v Chrysler Canada Limited[15] and Motherwell v Motherwell.[16]

In Krouse, the plaintiff sued for damages, claiming an invasion of his privacy by the defendant's use of unauthorized photographs of the plaintiff. In refusing an interlocutory application to strike out the statement of claim on the ground that it disclosed no cause of action, Parker J held:

> It may be that this action is novel but it has not been shown to me that the court in this jurisdiction would not recognize a right of privacy.[17]

The trial judge in Krouse, Haines J, found for the plaintiff on other grounds (appropriation of personality, breach of confidence, unjust enrichment) but obiter held that determination of such a fundamental pronouncement of law, as a tort of privacy, ought to be left to a higher court, unless essential to the case at hand.[18]

It is submitted, therefore, that Krouse does little to advance the enactment of a tort of privacy in

Canada. It was a decision of the Ontario High Court and, as observed by Haines J,[19] such a fundamental change in the law should be made by a higher court. Further, the application to strike out the plaintiff's claim was an interlocutory one, where the burden on the applicant was onerous - to show that there was no reasonable cause of action. Parker J in Krouse, observed that the power to strike out a statement of claim should be used sparingly and in the circumstances only if there was a binding precedent declaring no tort of privacy.[20] As he found no such precedent, he held that the plaintiff had a right to be heard at trial. This is very different from suggesting that a common law right of privacy exists, or even should exist, in Ontario. The decision is based on the burden of proof in the particular application.[21]

A second case that is also commonly regarded as supporting the creation of a tort of privacy is that of Motherwell v Motherwell.[22] The issue before the Alberta Court of Appeal was whether or not harassing telephone calls constituted undue interference with the comfort and enjoyment by the plaintiffs of their property. The court, in holding that it did, rejected the argument that invasion of privacy and nuisance were separate concepts and held that invasion of privacy, by prolific and persistent harassment of the plaintiffs in the home by use of a telephone system, was within the principle of private nuisance.[23]

The relevance of this case to the law of informational privacy is very limited. The court defined invasion of privacy narrowly, referring only to unwanted communications,[24] and specifically excluding all other forms of surveillance. The decision is therefore not directly relevant to informational technology. Even in the area of nuisance, the decision was not breaking new ground. Earlier Australian cases of Stoakes v Brydges[25] and Alma v Nakir[26] had granted a remedy in nuisance for "torture by telephone". These earlier cases did not prompt any fusion of the law of privacy and nuisance, and it would therefore seem unlikely that Motherwell could cause such an effect. Lastly, the judgment in Motherwell was specifically related to an area of the law of nuisance which happened to involve an aspect of privacy. It did not have any direct reference to privacy per se.[27]

Only in one case in Canada has a plaintiff succeeded on the grounds of an invasion of his privacy by the defendant. In Saccone v Orr,[28] the defendant recorded his telephone conversations with the plaintiff and then, in breach of an undertaking, divulged these recordings. Jacob Co Ct J. held that in such circumstances the plaintiff "must be given some right of recovery for what the defendant has in this case done" and gave judgment on the ground of invasion of privacy.

This authority is very dubious. It was made only at the County Court level. There was no examination of the law of privacy. The case, properly analyzed, appeared to involve a breach of confidence. Jacob Co Ct J. referred to the breach of confidence by the defendant in divulging the conversation, but did not base his decision on this point.

It may be that a constitutional recognition of privacy under the Charter will provide some impetus for a recognition of the right at common law.[30] Gibson argues that some charter violations, not in themselves torts, can give rise to tortious liability because of the wide discretionary remedies available under s.24(1) of the Charter.[31] He also argues that tortious liability is imposed through the inherent right of a superior court to award a remedy where none exists.[32] (ubi ius, ibi remedium) Gibson cites two cases,[33] Bertram S. Miller Ltd. v The Queen[34] and Crossman v Queen[35] where damages have been awarded for Charter violations.

As we shall see later,[36] a general right of privacy has not be recognized in s.7 of the Charter, although s.8, which deals only with the acquisition of information, has recognized a right of privacy, including informational privacy. If a general right of privacy is recognized in the Charter, it may be one reason for the courts to consider a change of policy and recognize privacy at common law.

Even if a right of privacy at common law is declared, its effectiveness as a means of controlling the informational practices of government institutions is likely to be minimal.

It is by no means certain that a common law right of privacy would include a right to informational privacy, giving rise to potential liability of government institutions in relation to their handling of information. The cases where a right of privacy has been discussed, such as Saccone, Motherwell and Krouse, all involved a physical and obviously wrongful intrusion into the individual's life.[36] If the courts are concerned by the uncertainty created by a recognition of a new tort (as suggested by Dixon J. as he then was, in Victoria Park Racing Co. v Taylor[37]), then they will limit the application of the doctrine, at least initially, to obvious abuses.

Further, torts are private actions in which the plaintiff carries the onus of proving his claim and financial loss.[38] In many instances it would be difficult to establish a wrongdoing on the part of government institutions. For example, if information is voluntarily supplied by an individual, then the use of the information by the government institution would not create a wrongful act giving rise to liability.[39] Establishing financial loss may also be difficult, especially when the information had no commercial value. The individual would therefore have to choose whether or not to conduct an expensive and public court action, when the likelihood of being awarded anything other than normal damages was remote.[40]

Lastly, a common law right of privacy would not assist the individual in obtaining access to information whereby he could establish that a wrong had been perpetrated by a government institution. The individual is left unaware of potential infringements.

In summary, a common law right of privacy would be uncertain in its application, difficult to prove, unlikely to award anything other than nominal damages, and difficult to ascertain when the right might be exercised. Therefore, although in theory a government institution is subject to a possible claim for damages, the reality would be that such claims would only be successful in a very small number of cases. Vis-a-vis government institutions and their informational practices, the individual would have been given an illusory right. As such, the declaration of such a right would be insufficient to instill in the individual a belief in the fair handling of information by government institutions.

## PART 3. REGULATION OF THE INFORMATION PROCESS BY COMMON LAW TORTS

### (1) Introduction

Despite the absence of a tort of privacy, various other common law torts are capable of exercising some control over the informational process. These torts fall into two categories.[41] First, there are those which are capable of imposing standards in the way government institutions handle information. Defamation, breach of confidence and negligence are the most relevant torts in this category.[42] Secondly, there are torts which, although not directly regulating the informational process, incidentally have the effect of restricting the acquisition of information. Trespass and nuisance fall into this category.[42a]

The effect both categories of torts have in protecting civil liberties will largely depend on their applicability to the informational practices of government institutions.

### (2) Defamation

The tort of defamation constitutes a restriction in the circumstances in which information can be transmitted. Defamation can be defined as "the dissemination of information that tarnishes the good name of a person causing his standing in the community to be impaired or causing him to be pitied."[43]

The potential impact of defamation on the governmental information process lies in that if government institutions issue defamatory statements, the defamed individual is able to bring an action for damages.[44] A check is therefore provided on government institutions using speculative or unsubstantiated information.[45]

However, in practical terms, the impact of defamation on the modern informational process is limited. Defamation requires publication as an essential element.[46] It is unclear whether this element of publication is satisfied when an official of a government institution merely retrieves a piece of information from a computerized databank. In R v McLaughlin,[47] referred to previously, it was held that a computer did not transmit, emit or receive information, but rather it performed an internal retrieval function. One could therefore argue that there has been no publication, and hence no defamation, when an operator on a computer terminal transmits false information within the institution.

There is some support to this argument from defamation cases.[48] In Mims v Metropolitan Life Insurance Co.,[49] the United States Court of Appeal (2nd circuit) held that the dictation by a corporate officer to a stenographer also employed by the same corporation, did not constitute publication as there was not third party receiver of information. The English case of Brayanston Finance Limited v DeVries[50] reached the same result, although the court held that there was publication but that it was protected by the qualified privilege of the common interests of business to get the letter written.

These cases do suggest (when read with McLaughlin), that a strong argument can be advanced that the use of a databank by an employee of a particular government institution does not constitute publication of that information.

Whether there is publicaton is also doubtful in the case where the official of a government institution obtains information, through linkage, from the databanks of another institution. On the one hand, a defamed individual would argue that the decisions in Mims and Brayanston Finance are distinguishable in that here there has been communication to a third party[51] and not merely internally within the corporation or institution. Such a position would seek to distinguish McLaughlin on the basis that it was a criminal case and that a more liberal interpretation of the computer's function should be adopted in the civil sphere.

On the other hand, as well as relying on McLaughlin, one could argue, on the basis of the doctrine of the Crown being one and indivisible,[52] that a communication between government institutions is not a communication to an external third party, but rather an internal communication within the Crown in its separate identities. It is clear, however, that this argument could apply only in respect of institutions of the same government, as the doctrine recognizes separate Crowns of each province and the federal government.[53]

The numerous defences to a defamation action will also ensure that this tort provides only minimal protection to the individual against informational practices of government institutions. First, truth is an absolute defence to a defamation action.[54] However, the modern information enables government institutions to acquire and use far more information about individuals. As we discussed previously, often it is the use of true information that is of concern. The defence of truth ensures that the tort of defamation will not be able to allay this concern.

The scope of qualified privilege further emasculates the effect of defamation in this area. Qualified privilege arises:

> where the person who makes the communication has an interest or a duty, legal, social or moral, to make it to the person to whom it is made and the person to whom it is so made, has a corresponding interest or duty to receive it.[55]

There are three categories of this privilege relevant for present purposes. First, the privilege arises when the information is conveyed, pursuant to a public or private duty, legal or moral, to someone who has a reciprocal interest in receiving it.[56] A moral duty is found if recognized by "people of ordinary intelligence and moral principle, but at the same time not a duty enforceable by legal proceedings".[57]

It may be difficult to find a legal duty on the part of government institutions to convey information to another institution. Section 8 of the Privacy Act, for example, gives the head of a government institution a discretion whether or not to convey information in the prescribed circumstances.[58] However, a moral duty may be easier to find. If the institutions share a common interest, for example law enforcement, then it may be that such a common interest imports a moral duty to share information.[59] Although section 8 of the Privacy Act falls short of imposing a legal duty, it does suggest that information will and should be shared amongst institutions. For example, section 8(e) suggests that information will be supplied to law enforcement agencies on written request. Even in the absence of a specific common purpose, if one accepts that government institutions together form a part of the indivisibility of the Crown, then it may be that the general common interest of efficient and non-discriminatory performance of duties is sufficient to imply a moral duty to share information.

The second category of qualified privilege (and closely related to the first) arises when the communication is made on a subject on which the communicator and the recipient share a common legitimate interest.[60] It therefore protects discussions between parties about matters of mutual concern (such concerns might be economic, as in the case of a company meeting, or might be trade or professional, as in the case of disciplinary proceedings against a member).[61] Again, where there is a specific common purpose between institutions (eg. law enforcement), then the common legitimate interest required for this privilege is easy to find. (eg. sharing information about suspects of a crime). However, if the argument is accepted that government institutions share a certain common purpose, then it may be possible to evoke this privilege in respect of most of the information that is conveyed by one institution to another.

Lastly, there is a limited privilege of communications in the public interest, commonly associated with matters such as reporting offences to the police etc.[62] Recent cases have expanded the circumstances in which this privilege can be claimed and it now appears that a government official who makes a defamatory statement about matters of general public interest[63] (eg.

misuse of funds etc.) will be protected. Further, individuals have been protected by this privilege when making defamatory statements to a government institution concerning matters which are within the jurisdiction of that institution.[64] If one finds the public interest in such cases is the bringing of appropriate matters before the institution concerned, it should be irrelevant whether that information is supplied by an individual or another government institution. A further major limitation of defamation is that the individual is unaware that a defamatory statement has been made. As demonstrated previously, informational technology has increased the anonymity and secrecy of government institutions. The individual is unaware what information has been acquired and where it has been disseminated. He bears the burden of proving that a defamatory statement has been made. In context of the informational process, he must trace the information from one databank to another, and then relate the "publication" of the information to an injury on his reputation.[65]

Our conclusion must unequivocally be that defamation does not, and is not, capable of providing any meaningful protection to individuals against the advances in the informational process. Consequently, it possesses little likelihood of influencing the informational practices of government institutions. As the Ontario Law Reform Commission stated:

> At most all it (the tort of defamation) achieves is to ensure that government does its homework and only discloses true information about individuals.[66]

### (3) Breach of Confidence

Breach of Confidence also has a direct impact on the informational process. The Younger Committee Report stated:

> this remedy protects privacy as such more than any other and recommended that the Law Commission examine this area of the law with a view to its clarification and statement in legislative form.[67]

The potential impact of breach of confidence on the informational process of government institutions lies in that it imposes certain standards in relation to the handling of information. Government institutions must respect the purpose for which the information was supplied and not disclose it to another person or individual for another purpose.

Although there has been considerable debate,[68] it now appears fairly settled that the basis of breach of confidence lies in equity. As Lord Denning stated in Seager v Copydex, it (breach of confidence):

> does not depend on any implied contract. It depends on the broad principle of equity that he who receives information in confidence, shall not take unfair advantage of it. He must not make use of it to the prejudice of he who gave it without obtaining consent.[69]

This was accepted by the Supreme Court of Canada in Slavutych v Baker[70]. More recently in R v Stewart,[71] the Surpeme Court, in considering breach of confidence under the Criminal Code,[72] reviewed the authorities of breach of confidence in the civil context and held that no Canadian court had conclusively decided that confidential information included a proprietary interest. The Court instead followed the Seager line of authorities (i.e. equitable basis to breach of confidence). Lamer J, in delivering the judgment of the Court, did find that it was possible, with time, that confidential information, in the civil context, may get to the stage where it is considered as property.[72]

If it does reach this stage, then the individual may be able to use breach of confidence to impose further restrictions on the use of confidential information by government institutions. For example, the individual with property rights, could presumably request the return of the information. The rights of the "owner of the information" vis-a-vis third party recipients of the information, even if bona fide and for value, may also be stronger.[73]

However, in the context of the informational process of government institutions, it will often be difficult for an individual to establish that a breach of confidence has occurred.[74] Megarry J in Coco v A.N.

Clarke[75] set out three criteria for a breach of confidence action to succeed. They were:

(i) The information must have "the necessary quality of confidence about it".[76]

(ii) The information must have been imparted in circumstances imposing an obligation of confidence.

(iii) There must be an unauthorized use of the information to the detriment of the party communicating it.[77]

Each of these criteria pose difficulties to the individual when suing a government institution for breach of confidence.

It is clear that personal information does satisfy the first of the above criteria, namely having the requisite degree of confidentiality.[78] More doubtful, however, is the status of information created through the associational techniques of computers in combining various pieces of information to create a new item of information. In such situations each individual piece of information may not be confidential, although the "new information" may be of a confidential nature. However, going back to the basis of the doctrine, as established in Seager v Copydex,[79] it would appear doubtful that this new information has been received in confidence by the government institution, but rather it has been created by that institution.

In attempting to establish the second criteria, the individual will argue that he supplied the information for a limited purpose (eg. receipt of a benefit or service) and the receipt of that information by the government institution was sufficient to imply the existence of a confidential relationship in respect of that information.[80] This seems to have been accepted in Norwith Pharmacal Co. v Commissioners of Customs and Excise,[81] where the court, in refusing to order the Commissioner to divulge the names of various importers to the plaintiff (so that it could commence an action against those importers for infringement of copyright), held that the names had been supplied to the Commissioner by the importers in confidence. Thus, a confidential relationship between the individual supplying the information and the government is recognized. In Butler v The Board of Trade[82] it was also recognized that, in the circumstances, the Board of Trade was a recipient, although an innocent one, of confidential information.

However, not always will a confidential relationship exist when a government institution acquires personal information from an individual. In Malone v Metropolitan Commissioner of Police (No. 2),[83] the plaintiff, acquitted from the charge of stolen goods, brought an action against the police alleging, inter alia, breach of confidence by recording telephone communications of the plaintiff. Although Megarry V-C, in dismissing the claim, could have relied on the public interest defence of the police, he went further and found that, in the circumstances, there was no confidential relationship. Rather, the person who imported the confidence must expect to have their conversation recorded. If this decision is followed in Canada, it would virtually render inapplicable the doctrine of breach of confidence where information is gained by government institutions from direct personal surveillance of individuals. Subsequently, in Francome v Mirror Group Newspapers Ltd.,[84] Malone was distinguished on the basis that it referred only to authorized tapping by police and not illegal tapping by private parties. The plaintiff could therefore succeed in any action for breach of confidence. Government institutions, not being law enforcement agencies, fall somewhere between the above two categories.

Even if confidential information is imparted and a confidential relationship is established, a government institution may be able to rely on the defence that it breached a duty of confidence in the public interest.[85] At the minimum, this defence would apply to cases where there has been wrongdoing on the part of the party seeking to restrain the use of confidence.[86]

However, the public interest defence appears to go further and involve the weighing of the public interest in each case, irrespective of wrongdoing.[87] Thus in Hubbard v Vosper,[88] it protected disclosure of information relating to practices dangerous to mental health.

What is crucial in the informational context is establishing how widely the public interest defence can be used to protect government institutions who divulge confidential information to another such institution. In particular, whether it can apply to all cases where the information has been disclosed to further the performance of duties by the government institution which receives the information. In such a case, one could argue that it is in the public interest that the confidence be disclosed.[89] There are no decided cases on this point. The Ontario Law Reform Commission found that:

> the extent to which the Ontario government might be able to take advantage of the established defence of public interest is unclear.[90]

Establishing the requisite degree of detriment to found an action and obtain a suitable remedy will also present difficulties to the individual suing a government institution. Clearly the individual is entitled to damages for breach of confidence.[91] However, an individual will often not suffer direct financial loss by a government institution breaching confidentiality by transmitting personal information to another government institution. Only if it could be established that a different decision would have been reached if the confidential information had not been used, is this individual likely to have sufficient financial loss.

Other remedies available for breach of confidence including a delivery up of goods or their destruction or an accounting of profits, are commercial remedies concerning the exploitation of a product and have no relevance to the informational process of government institutions.

An injunction is normally available for breach of confidence, both against the original party breaching the confidence and against subsequent recipients.[92] In granting an injunction in Argyll v Argyll,[93] the court applied the test of whether the newpaper ought reasonably to have known that the information had been supplied in breach of confidence.

The individual, however, will find it difficult to obtain an injunction against the Crown (or a government institution who enjoys the same immunities and privileges of the Crown - ie. which are agents of the Crown).[94] The common law position is that no injunction is available against the Crown in the absence of an express statutory provision to the contrary.[95] Some exceptions do exist, and an injunction can be obtained against a crown officer who is shown to have acted illegally.[96] Statute law has not generally expanded the circumstances in which an injunction can be awarded against the Crown.[97]

It is apparent, therefore, that the action of breach of confidence has little relevance to the informational process of government institutions. The many obstacles discussed illustrate that breach of confidence is in essence a private remedy and hence is unlikely to effect informational practices. There have been no cases in Canada where the government has been sued for a breach of confidence.[98]

### (4) Negligence

An action for negligence may, in theory at least, lie where it can be proved that there has been some mishandling of personal information by a government institution.[99] If this action is readily available, government institutions will be forced to alter their informational practices so as to avoid liability. In doing so, some of the intrusions into civil liberties will be curtailed.

However, only in one instance has the government been held liable in respect of the negligent handling of information. In Barnes v Commonwealth,[100] the government was held liable in negligence for inaccurately notifying the plaintiff that her husband had been admitted to a mental asylum. The court in Barnes specifically rejected the notion that there was any general duty on the government not to disclose inaccurate information. Rather, the duty arose out of the specific circumstances of that case and the reasonably foreseeable injury to the plaintiff[101] (who was an old widow and suffered nervous shock on receiving the notification).

It follows from the decision in Barnes, that it will be difficult to establish that government institutions owe any more general duty of care in respect of the handling of information. If the only duty is not to disclose false or inaccurate information, then the impact on the informational process will be minimal. For example, no duty would lie concerning the dissemination of true information[102] or ensuring that decisions are made using accurate information.

Further, the requirement that there must be some degree of physical harm (or nervous shock), before a duty is owed further restricts the use of negligence in this area.[103] Pure economic loss resulting from the use or disclosure of false information by a government institution would be unrecoverable. There is some evidence of a modification of this doctrine. In Rivtow Marine Limited v Washington Iron Works[104] the Supreme Court of Canada allowed compensation for purely economic loss, provided it resulted from directly and demonstrably foreseeable negligence. It is far from clear how the standard will be interpreted (one interpretation requires the defendant, before it is liable to the plaintiff, to have actual knowledge of the risk to the plaintiff),[105] but if it is more broadly interpreted, as appears likely,[106] one restriction in making government institutions liable in negligence for the mishandling of information will be removed.

The immunity of government institutions from civil liability when exercising legislative or quasi-judicial duties further restricts the situations where a duty of care can be imposed.[107] While it is obviously a question of fact in each case whether a government institution is exercising such a function, it will, at least in some instances, shield them from liability.

Even if a duty of care is established, the individual will face a further hurdle in proving that there is a breach of that duty. The burden of proof is clearly on him to establish negligence on the part of the government institution in relation to the handling of information. It is at this stage (i.e. considering whether there has been a breach of duty), that a court would consider what standards ought to be imposed on government institutions. For example, questions such as what checks should be made to ensure that only accurate information is gathered and whether the individual should be notified when information is being used, would be considered.

Lastly, the individual will have the difficulty, in common with other torts, of establishing that he has suffered financial loss justifying an award of damages.

### (5) Trespass

The law relating to trespass has had a significant historical impact on the acquisition of information. Some form of physical intrusion onto land was often necessary to acquire personal information about an individual.[108] The law of trespass, however, prevented any unauthorized intrusion with the result that far less personal information about individuals was collected.

The impact of trespass today is not significant. Trespass can be defined as the "unauthorized entry upon the soil of another".[109] The plaintiff must therefore prove both a physical entry and an unauthorized entry. However, informational technology has made physical penetration of soil unnecessary to acquire information (eg. by use of the parabolic microphone and the other devices discussed in Chapter II). Further, the law of trespass is irrelevant to the ability of government institutions to acquire information from other sources such as through the sharing of information with other institutions or the recording of information supplied by an individual or third party.

The second element of trespass, unauthorized entry, is also difficult to establish. Government institutions have generally broad powers to intrude onto an individual's property.[110] For example, we have referred previously to the powers of search and seizure and entry onto premises by law enforcement agencies under the Criminal Code.[111] Departments administering welfare benefits have similarly broad powers,[112] often it is argued that a pre-requisite to the obtaining of benefits is the voluntary abandonment of privacy.[113]

Although trespass does have the advantage over the torts previously examined, that no proof of damages is required, if in fact no damage is suffered, then it is likely that only nominal damages will be awarded.[114]

Trespass to chattels or personal property has the same basis as trespass to land, but instead deals with unauthorized interference with a chattel in possession.[115] It therefore applies when information is acquired through intereference with a chattel. An obvious example would be where a listening device is implanted in a car.[116] Trespass to chattels is subject to the same limitations as trespass to the land.

### (6) Nuisance

Like trespass, nuisance, although its primary purpose is to protect an interest in land, may incidentally restrict the acquisition of information. Private nuisance is "an unreasonable intereference with the use and enjoyment of the land".[117] It is distinguishable from trespass in that there need not be actual physical intrusion of the land affected.[118] However, the courts have generally held that there must be some physical interference with the land. Thus in Victoria Park Racing Co. v Taylor,[119] the court held that there was no nuisance when the defendant observed and broadcast from a tower on adjacent land races being conducted on the plaintiff's land.[120]

However, the categories of nuisance are not closed,[121] and there are some indications that the courts are expanding the doctrine in such a way as to have relevance to the informational process by making actionable certain forms of surveillance and intereference with the plaintiff's property.[122] In Motherwell v Motherwell,[123] referred to previously, the Court of Appeal of Alberta extended the scope of nuisance to include the specific act of harassment by telephone. However, the court was careful to stress that only this act should be considered a part of nuisance and general acts of surveillance and acquisition of information should not be so considered.[124]

The doctrine of "watching and besetting" as reaffirmed in Poole v Ragen and Toronto Harbour Commission,[125] also imposes a limit on the surveillance power of government institutions. In that case, the police followed the plaintiff's boat back and forth across Toronto Harbour for a period of three months. It was held that such actions constituted interference with the enjoyment of one's private life and personal freedom. As such, it was an "affront to the dignity of any man" and an actionable nuisance, unless justified.[126]

The importance of both these decisions is that they indicate that the court may be willing to expand the scope of nuisance and include within its categories some form of unreasonable surveillance.[127] However, in each case the court was careful not to expose any general theory of protection. In Motherwell the protection was limited to prevention of harassment by telephone; in Poole by the "watching and besetting" principle ("watching and besetting prevents surveillance calculated to compel the plaintiff into a particular course of action").[128] A crucial element in this theory is the plaintiff's knowledge of the surveillance. Such a requirement is a severe limitation in the area of modern information technology, as much surveillance is carried on without the plaintiff's knowledge. Nevertheless, nuisance is a more flexible tort than trespass. The "interference" required in nuisance is far broader than the requirement in trespass of intrusion.

However, the effectiveness of nuisance as a remedy against modern informational technology is limited. First, with the exception of the watching and besetting principle, nuisance requires some form of interference with the enjoyment of the land. Most surveillance and acquisition of information need not interfere with any such enjoyment. Secondly, the plaintiff must have an interest in the land.[128] Thirdly, the plaintiff will again bear the burden of proof of the occurrence of some form of nuisance and also that he suffered some injury, an essential ingredient of nuisance.

## (7) Conclusion

One basis as to how common law torts protect civil liberties is that they identify the point beyond which the exercise of State power (in this case over information) is not legal. The right to sue the government is the means the individual has to enforce this obligation. Therefore, if officials perceive that government informational practices are likely to expose the institution to a law suit, they will alter such practices so as to not cause an infringement. Consequently, the intrusion into the individual's liberty would be restricted.

In the cases of torts which can directly regulate the use of information, one can see how this theory works. For example, if a negligence action laid down rules as to what constituted a breach of duty by government institutions in relation to the handling of information, then it would be quite conceivable that government institutions would alter their practices so as to come within such rules. Similarly, standards could be imposed by the court through the breach of confidence doctrine and defamation in relation to the disclosure of information.

However, in practice the common law torts are incapable of producing this result. There is often difficulty in applying these concepts to the informational practices of government institutions. We have seen, for example, the difficulties of proving a confidential relationship, of establishing "publication" for the purposes of defamation, and of establishing a duty of care in negligence. Further, many defences can be used by government institutions. Truth and qualified privilege are examples in the area of defamation, as is public interest in breach of confidence. Lastly, there is the difficulty of proving the government institution was at fault and that the individual suffered financial loss as a consequence.

These limitations of using tort remedies against government institutions make it impossible to predict with any confidence the point where State power over information ends. Therefore, standards regulating the informational process are not able to be imposed by the courts on government institutions. Accordingly, the infringement of civil liberties goes unchecked.

As the use of information cannot be a central element of torts, such as trespass and nuisance, then potential protection of civil liberties from advances in informational technology is more limited. No general standards in relation to the handling of information can be imposed, but rather the physical ability of government institutions to acquire information is restricted. Consequently, the number of intrusions into civil liberties is also restricted.

This theory is also unworkable in practice. Government informational practices simply do not need to infringe the concepts of trespass and nuisance to acquire information.

## FOOTNOTES - CHAPTER III

1. Mann "Britain's Bill of Rights" (1978) 94 *L.Q.R.* 512, 512 quoting Blackstone "*Commentaries on the Laws of England*", 6.

2. Ibid.

3. Lester "Fundamental Rights: The United Kingdom Isolated" (1984) *Public Law* 46, 46 quoting Dicey "*An Introduction to the Study of the Constitution*" (10th ed., 1959), 145.

4. Lester Ibid 47.

5. Section 26 of the Charter specifically provides that existing rights or freedoms are not denied by enunciation of the protected rights.

6. eg. Braithwaite "The Effect of Section 8 of the Canadian Charter of Rights and Freedoms on Section 10 of the Narcotic Control Act" (1984) 48 *Sas. L.R.* 231.

7. Supra at p.3.

8. Fridman *Introduction to the Law of Torts* (1978), 164; see also Geddes "The Private Investigator and the Right to Privacy" (1989) 27 *Alta. L.R.* 256, 286. Burns "The Law and Privacy. The Canadian Experience" (1976) 54 *Can. B.R.* 1, 12. The case frequently quoted in support of this contention is *Victoria Park Racing Co.* v *Taylor* (1937) 57 CLR 479, 496 where Latham CJ held "Neither this Court nor a court of law will interefere on the mere ground of invasion of privacy".

9. Burns Ibid 12 citing Fleming *The Law of Torts* (4th ed, 1971), 526-527.

10. Ibid.

11. Dworkin "The Common Law Protection of Privacy"

(1967) 2 U of Tasmania L.R. 418, 436.

12. (1937) 57 CLR 479, 505 quoted by Dworkin Ibid.

13. See Bailey Harris Jones Civil Liberties: Cases and Materials (2nd ed, 1985), 4 quoting Street Freedom, The Individual and the Law (5th ed., 1982) 263.

14. See eg. Lord Denning in Re X (a minor) (I1975) 1 All ER 697, 704. "We have as yet no general remedy for infringement of privacy: the reason being that on balance it is not in the public interest that there should be."

15. Supra at p.11 ff.

15a. (1970) 12 D.L.R. (3rd) 463.

16. (1977) 73 DLR (3rd) 62. For a discussion of these cases see Burns supra n8 at p12. Ontario Commission on Freedom of Information and Individual Privacy Vol 3 Protection of Privacy (1980), 214.

17. (1970) 12 D.L.R. (3d) 463, 464. See also Burnett v The Queen in Right of Canada (1979) 94 D.L.R. (3d) 281, 288 where an application to strike out a statement of claim alleging privacy also failed.

18. (1972) 25 D.L.R. (3rd) 49, 68.

19. Ibid 56.

20. (1970) 12 D.L.R. (3rd) 463, 464.

21. Ibid.

22. (1976) 73 D.L.R. (3rd) 62.

23. Ibid 74.

24. Ibid 67.

25. [1958] Q.W.N. 5 quoted in Dworkin Ibid.

26. [1966] N.S.W.R. 1173.

27. Geddes supra n8 at 286 refers to Capan v Capan (1981) 14 C.C.L.T. 191 which followed Motherwell.

28. (1981) 34 O.R. (2d) 317. The same is not true of the Law of Quebec. See Glenn "The Right to Privacy in Quebec Law" in Gibson "Aspects of Privacy Law - Essays in Honour of John M. Sharp" (1980) 41 who refers to Robbins v CBCB (1957) 12 D.L.R. (2nd) 34 and at 1053 of Quebec Civil Code.

29. (1981) 34 O.R. (2d) 317, 322.

30. Gibson "Tort Law and the Charter of Rights" (1987) 16 Manitoba L.R. 1,2.

31. Ibid.

32. Ibid 3.

33. Ibid.

34. (1985) 18 D.L.R. (4th) 600.

35. (1984) 9 D.L.R. (4th) 588.

36. Infra at p.194.

37. Supra n8.

38. Ontario Commission on Freedom of Information and Individual Privacy, supra n16 at 220.

39. i.e. it is not reprehensible conduct, to use Fleming's terminology; supra n9.

40. Ontario Commission on Freedom of Information and Individual Privacy, supra n16 at 220.

41. See Williams "Invasion of Privacy" (1973) 11 Alta. L.R. 1, 6.

42. Ibid. See for a discussion of these torts Geddes supra n8 at 273 ff; Burns supra n8 at 12 ff. Ontario Law Reform Commission on Freedom of Information and Individual Privacy, supra n16 at 134 ff.

42a. Ibid.

43. Fleming The Law of Torts (6th ed., 1973), 568; Substantially similar definitions are made by Linden Canadian Tort Law (4th ed., 1988) 628; Canadian Encyclopaedia Digest (Western) (3rd ed.) Vol 11a, 35 citing Thomas v C.B.C. [1981] 4 W.W.R. 281.

44. McLaughin "Education Records and the Right to Privacy" (1981) 15 U.B.C.L.R. 175, 82.

45. Ibid.

46. See for example Linden supra n43 at 644. Canadian Encyclopaedia Digest (Western) supra n43 at 63.

47. (1981) 113 D.L.R. (3rd) 386.

48. See Linden supra n43 at 644, n135 for reference to the following cases.

49. (1952) 200 F (2d) 800.

50. (1975) 1 Q.B. 703.

51. Thus bringing it within the principle of Lawrence v Finch [1931] 1 D.L.R. 689 where dictation by an employer to an employed stenographer did constitute publication because she was held to be a third party.

52. See Hogg Constitutional Law of Canada (2nd ed., 1988), 216.

53. Ibid.

54. Linden supra n43 at 649; Canadian Encyclopaedia (Western) supra n43 at 83.

55. Linden Ibid 658 citing leading case in this area being Adam v Ward [1917] A.C. 309.

56. Linden Ibid.

57. Ibid.

58. Privacy Act S.C. 1980-81-82-83, c111, section 8 "Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed ..."

59. Linden supra n43 at 659 refers to the example of mercantile agents who share information not for profit. They attract qualified privilege - see London Assoc. for the Protection of Trade v Greenlands [1916] 2 A.C. 15.

60. Linden Ibid 656.

61. Ibid.

62. Ibid 660. See also Fleming supra n43 at 529.

63. Linden Ibid citing Stopforth v Goyer (1979) 8 C.C.L.T. 172, and Parlett v Robinson (1986) 37 C.C.L.T. 281.

64. Ibid citing Wilcocks v Howell (1884) 5 O.R. 360; Latta v Fargey (1906) O.W.R. 231.

65. Washburn "Electronic Journalism, Computers and Privacy" (1981) 3 Computer L.J. 189, 204 makes this point re application of torts generally.

66. Ontario Law Reform Commission on Freedom of Information and Individual Privacy supra n16 at 229.

67. Report of the Committee on Privacy, CMND 5012, 1972 (Younger Committee), para.87.

68. See R v Stewart (1988) 50 D.L.R. 1, 10 where Lamer J cites the numerous cases supporting particular basis for breach of confidence.

69. [1967] 2 All E.R. 415; See also Fraser v Evans [1969] 1 All E.R. 8 where Lord Denning affirms Seager v Copydex.

70. (1975) 55 D.L.R. (3rd) 229, 230.

71. (1988) 50 D.L.R. 1, 10. For a discussion of R v Stewart pre the Supreme Court decision see Weinrib "Information and Property" (1988) 38 U of Toronto L.J. 117.

72. Criminal Code section 283(1) (rep. & sub 1974-75-76, C93) "Everyone commits theft who fraudulently and without colour of right converts to his use or to the use of another person, anything whether animate or inanimate."

72a. (1988) 50 D.L.R. 1, 10.

73. Cornish Intellectual Property (2nd ed., 1989), 260.

74. McLaughlin "Education Rights and the Right to

Privacy" (1981) 15 U.B.C.L.R. 176, 181.75.[1969] R.P.C. 141.

76. Quoting Lorde Greene in Saltram Engineering Ltd. v Campbell Enginering Ltd. (1948) 65 R.P.C. 203.

77. [1969] R.P.C. 141.

78. Cornish supra n73 at 220.

79. Supra at n69.

80. Cornish supra n73 at 231 citing Butler v Board of Trade. (see note 82) and Norwich Pharmaceutical Co. v Commissioner of Customs and Excise (see note 81).

81. [1973] 2 All E.R. 943.

82. [1970] 3 All E.R. 593. In this case, the Board of Trade innocently on a liquidation, came into possession of a letter written by the solicitor to the defendant warning of consequences if the defendant undertook a certain cause of action.

83. [1979] 2 All E.R. 620.

84. [1984] 2 All E.R. 408.

85. See generally Cornish supra n73 at 224 and also Norwich Pharmaceutical v C.C.E., supra n81.

86. Norwich Pharmacal v C.C.E., Ibid 766. See also Ontario Commission on Freedom of Information and Individual Privacy, supra n16 at 188.

87. Cornish supra n73 at 224. See also Norwich Pharmacal v C.C.E., supra n81.

88. [1972] 1 All E.R. 1023.

89. See Ontario Commission on Freedom of Information and Individual Privacy, supra n16 at 190.

90. Ibid 229.

91. See _Argyll_ v _Argyll_ [1965] 1 All E.R. 611.

92. Ibid 627.

93. Ibid.

94. Hogg, supra n52 at 219.

95. Spry _Equitable Remedies: Injunctions and Specific Performance_ (1st ed., 1971) 312.

96. Ibid 313.

97. See Hogg, supra n52 at 223.

98. Ontario Commission on Freedom of Information and Individual Privacy, supra n16 at 190.

99. Dworkin "The Common Law Protection of Privacy" (1976) 2 _U of Tas L.R._ 418, 443.

100. (1937) 37 S.R. (N.S.W.) 511.

101. Ibid 516.

102. See Ontario Commission on Freedom of Information and Individual Privacy, supra n16 at 179.

103. Burns, supra n8 at 20.

104. [1973] 6 W.W.R. 692. See Linden, supra n43 at 386 ff. for a discussion of this case.

105. Linden Ibid 389.

106. Ibid.

107. Ibid 415 quoting Welbridge Holdings Ltd. v Metropolitan Co. of Greater Winnipeg (1971) 22 D.L.R. (3rd) 470.

108. Burns, supra n8 at 14.

109. Ibid citing Blackstone's Commentaries, Vol. 3, p209.

110. Supra at p31.

111. Ibid.

112. Infra Chapter VI Part 3.

113. Shattuck "Rights of Privacy" (1977), 182.

114. Burns, supra n8 at 15.

115. Ontario Commission on Freedom of Information and Individual Privacy, supra n16 at 156.

116. Ibid.

117. Linden, supra n43 at 500.

118. Dworkin, supra n11 at 423.

119. (1937) 58 C.L.R. 479.

120. Followed in Canada. See Geddes, supra n8 at 276 citing In Re Copeland (1972) 28 D.L.R. (3rd) 26.

121. Dworkin, supra n11 at 423.

122. Burns, supra n8 at 18.

123. (1976) 73 D.L.R. (3rd) 62.

124. Ibid 74.

125. [1958] O.W.N. 77.

126. Ibid.

127. Burns, supra n8 at 24.

128. Ibid 17.

129. Dworkin, supra n11 at 425.

# CHAPTER IV - FEDERAL LEGISLATION

## PART 1. INTRODUCTION

The inability of the common law to protect civil liberties from advances in informational technology clearly predicates the need for some form of legislative initiative. Such an initiative could protect civil liberties in two ways. First, it might create new rights over information which the individual could exercise against government institutions. Secondly, it might enact standards to be observed by government institutions when handling personal information.

One might predict that legislation is better equipped in the area of informational technology to protect civil liberties than the common law. Legislation is able to enact rights specifically related to the informational process, thereby avoiding the problems of the applicability of the common law to the informational process. Further, legislation is able to provide direct enforcement of a framework regulating the handling of information by government institutions, whereas the common law must rely on legal action, or the threat thereof, to bring about a change in the informational process.

At the federal level, the enactment of the Privacy Act[1] is the main legislative response of the Federal Government to the threats caused by advances in informational technology.[2]

The companion act to the Privacy Act, the Access to Information Act,[3] complements this purpose. It provides access to public information, whilst the Privacy Act regulates personal information. Unrelated to these Acts, the Criminal Code, in reproducing the now repealed Protection of Privacy Act,[4] regulates electronic surveillance in Canada.

The effectiveness of these Acts in protecting civil liberties can be judged in terms of the new rights they give to the individual and the regulating effect they have on the informational process of government institutions.

## PART 2 - PRIVACY ACT

### (1) Application of the Act

At the outset, it is necessary to recognize a major restriction in the ability of the Privacy Act to satisfy civil libertarian concerns involving the use of information by government institutions. The Act only applies to those federal government institutions listed in the Schedule to the Act.[5] More importantly, the Act does not apply to provincial government institutions at all, although a review undertaken by a Parliamentary Committee has recommended the extension of te Act to these institutions.[5a]

In addition, certain government institutions are not listed in the Schedule to the Act, including Air Canada, Petro-Canada and Canadian National Railways, on the basis that they were organizations of a commercial nature.[6] Lastly, federal government agencies established after the commencement of the Act will not be covered until such time as their names are added to the Schedule.[7]

### (2) Scope of the Act

To properly analyze the Privacy Act, we must consider not only the actual rights and standards imposed in the Act, but also the approach it takes to solving the problems caused by advances in informational technology. The Act:

(i) Provides the individual with a right of access and correction of, personal information held in the databank of a government institution. Refusal of access is reviewed by the courts;[8]

(ii) Imposes certain self-regulatory restrictions on the way in which personal information may be collected, used and disclosed by government institutions;[9]

(iii) Provides for the indexing of information banks of federal government institutions;[10]

(iv) Does not create a right of privacy, but rather uses a purpose clause which states, inter alia, that the purpose of the Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves.[11]

(a) Right of Access in the Privacy Act

A strong right of access is essential if the civil liberties of individuals are to be protected from the advances in informational technology.[12] An individual is unable to form a belief in the fair handling of information when he is unaware of how information is being handled.

If the individual is freely able to ascertain the nature of the information held by the government institutions, the powerlessness caused by the informational process is diminished.[13] This effect occurs because a right of access can assist in preventing the anonymity of informational technology by making the individual aware of adverse decisions made by government institutions, the reasons those decisions were made, and the officer or institution responsible. Once provided with this information, the individual can consider what remedies he might employ to challenge these decisions.

In general, a free and loose relationship between government institutions and the individual is promoted.[14]

Further, a comprehensive right of access can have a beneficial effect on the overall standard of bookkeeping. Government institutions, aware of the greater accountability, will take better care that their decisions are able to withstand close scrutiny.

Pursuant to section 12 of the Act, individuals have a right, on request, to be given access to personal information held in the databanks of the institutions specified in the Schedule. Upon complaint by the individual concerned, any decision of a government institution to refuse disclosure is reviewed at first instance by the Privacy Commissioner, who acts as a mediator between two parties.[15] The Privacy Commission only possesses power to make recommendations.[16]. If this mediation is unsuccessful, the individual, or the Privacy Commissioner on his behalf, may apply for judicial review by the Federal Court.[17] Upon such review, the government institution bears the onus of proof to justify non-disclosure.[18]

However, the wide range of circumstances where access under the Privacy Act is not permitted, greatly erodes the principle of access. These can be grouped into three categories:

(i) Exemption of databanks from the Act;

(ii) Exclusion of databanks from operation of the Act;

(iii) Exceptions to the right of access, justifying non-disclosure by the head of a government institution.

(i) Exempt Databanks

Pursuant to section 18(1) of the Act, banks containing such information may be designated as exempt banks, to which the individual has no right of access. To be properly exempted, the files in such databanks must consist predominantly of information of the type described in sections 21 and 22 of the Act[19] (i.e. relating to defence or international affairs on law enforcement)

Twenty two banks have been exempted by Order of Council,[20] including all Royal Canadian Mounted Police databanks[21] and the Canadian Police Information Centre referred to previously.[22] The threat posed by law enforcement agencies is therefore in no way curtailed by the Privacy Act.

An individual has only limited rights of review against a refusal by the head of a government institution to disclose information held in an exempt bank. In Re Ternette and the Solicitor-General of Canada,[23] the court held that the extent of the review permitted by section 41 in those circumstances was to consider whether there was a file in an exempt bank, and if so whether the file was properly included in that bank. There is no power to order disclosure of that file.

However, it is open to debate whether even this limited review is permissible, and it may be that the only review permitted is an examination of the Order in Council declaring the bank be exempted.[24]

In Re Ternette, the court held that section 41 of the Act was unambiguous and that it provided a clear right for the individual to bring an application in any case where he was refused access.[25] Pursuant to section 48 of the Act, the court found that it was empowered to make the necessary orders, including a review of the particular file to see if it was properly included in the exempt databank.

The argument for a more restrictive approach, as a matter of statutory interpretation, appears equally strong. First, if an application is made pursuant to section 41 for review of non-disclosure, the court may make an order for disclosure pursuant to sections 48 or 49. However, before the court can make an order pursuant to section 48 (which was the relevant section in Re Ternette), it must determine that the head of the institution was not authorized under the Act to refuse disclosure. As section 18(2) expressly authorizes refusal in the case of all information in an exempt bank, then upon proving that the request involved a file in an exempt bank, the refusal must be authorized. Therefore, any further order that might be made under section 48 (such as the removal of a file) cannot be made because this initial test is not satisfied.

Secondly, Re Ternette did not consider the meaning of exempt in section 18(1) of the Act. Its natural meaning is "to grant a freedom or immunity"[26] - i.e. personal information in an exempt databank is immune from the individual's right of access. Section 12 supports this as it expresses the right of access to be "subject to this Act". Therefore, all information in exempt databanks is not subject to the right of access (and not just information properly included in the exempt databank).

Thirdly, the only express power in the Act to allow applications in respect of exempt databanks is provided by section 43, which is limited to applications by the Privacy Commissioner. Therefore, applying the expressio unius rule of statutory interpretation, a similar application by the individual is precluded. Although the court in Re Ternette rejected this argument (on the basis there was no ambiguity),[27] it is submitted the court failed to consider the effect of section 18 mentioned above, and section 51. Section 51 provides for the mandatory in camera proceedings of applications involving section 19 (confidential information received from other governments); section 21 (information from intelligence operations); section 43 (applications of the

Privacy Commissioner re exempt banks). The intention of section 51 must be to prevent any possible disclosure of sensitive information by making certain precautions mandatory. In a review initiated by an individual concerning a file in an exempt bank, similarly sensitive information would be involved. It is suggested that such a case is not provided for under section 51 because the drafters of the Act did not envisage that the individual had the power to make such an application in the first instance.

The Privacy Commissioner pursuant to section 36(1), may carry out investigation of files in exempt databanks and may, under section 43, apply to the court for the review of any file in an exempt databank. The court, under section 50, has the power to order removal of a file from an exempt bank.

The protection afforded by section 50 is, it is submitted, illusory. The activities described in section 21 and section 22 (matters relating to national security and law enforcement respectively) are defined so broadly that they, in all likelihood, can justify the inclusion of such files in an exempt bank. The Privacy Commissioner will probably be reluctant (as would be the courts)[28] to substitute his own opinion for that of a particular government institution as to what constitutes a matter invoking national security or law enforcement.

Further, the Privacy Commissioner has an absolute and unreviewable discretion in determining whether or not to carry out an investigation of an exempt bank. The wording of section 36,[29] and in particular the use of the words "may carry out an inspection from time to time", suggests that this discretion is exercised only pursuant to a general review of exempt banks, and not in relation to an individual complaint. Only if an individual file is discovered in the course of such a review to be wrongly included in the databanks can, it is suggested, the Privacy Commissioner apply for review by the court under section 43.

### (ii) Exclusion From the Operation of the Act

An even broader exception to the principle of access is provided by section 70, which excludes from the operation of the Act cabinet records of the last twenty years. Cabinet records are defined widely to include, inter alia background reports, memorandum, records relating to preliminary deliberations, and draft legislation.[30]

The effect of such a wide exemption is that it forestalls government accountability.[31] It helps ensure the anonymity of government institutions, thereby maintaining the imbalance of power between institutions and the individual.

It is unclear from the Act whether the mere claim that documents are cabinet records is conclusive, or if the courts have a limited power of inspection to determine that the records are properly classified as cabinet records.[32] There is no authority on this point, although cases involving claims of Crown Privilege do, by analogy, suggest that there may exist a limited power of inspection by the courts.

In Duncan v Cammell Laird,[33] the House of Lords held that a Ministerial Certificate stating that the documents were of a certain class and ought not to be produced on the grounds of public policy, was final and could not be reviewed by the courts. This decision has been rejected both in England[34] and in Canada.[35] It is now clear, as has been most recently held by the Ontario Court of Appeal in Re Carey and the Queen,[36] that in the absence of specific legislation confirming a right to absolute privilege, that a claim for Crown Privilege is only relative and the court is required to consider the relative weight of the Crown's claim for privilege and the other party's claim for disclosure. As Re Carey recognizes, and has also been explicitly held in Human Rights Commission v Attorney-General of Canada,[37] the legislation may prevent judicial review by making the privilege absolute and by expressly stating that no review is permitted by the courts.

It is submitted that section 70 of the Privacy Act is not absolute in these terms in that it does not specifically prevent review by the courts (eg. section 41(2) of the Federal Court Act,[38] considered in the *Human Rights Commission* v *Attorney-General of Canada* which stated "production shall be refused without any examination of the document by the Court"). If one accepts that section 70 is not absolute and that judicial review is permitted, then the substance of that review must be an examination of whether the document is of a type coming within the ambit of section 70. Such a conclusion would be in accordance with the spirit of cases invoking Crown Privilege, which promotes scrutiny of Ministerial claims.

Restrictions on the right of access (as provided by section 70) may be subject to scrutiny according to the Charter. If section 2(b) of the Charter, which guarantees freedom of expression, includes within its ambit freedom of access to information, then over-broad restrictions on this right of access in the Privacy Act may be invalid. Such scrutiny would apply to areas of total exemption to access as provided in sections 18 and 70 of the Act, and also to the exceptions set out in sections 19-28, which may be excessive. We will examine later in this paper the operation of section 2(b) of the Charter and its effect on the Privacy Act.

### (iii) Exceptions to the Right of Access

The many exceptions to the right of access set out in sections 19-28 of the Act constitute a third area of restriction of access to personal information. These exceptions either require mandatory non-disclosure or permit non-disclosure at the discretion of the head of the government institution.[39] A right of appeal does lie from such non-disclosure to the Privacy Commissioner pursuant to section 29 of the Act, who has the power to make recommendations.[40] If the individual is still dissatisfied after the investigation by the Privacy Commissioner, he may apply to the Federal Court for an order for disclosure.[41] The court may order disclosure if it is satisfied that the government institution was not authorized to refuse disclosure,[42] though if the matter involves federal-provincial affairs, international affairs and defence, law enforcement, or sentencing information, a stricter test is applied and the court must be satisfied that the head of the institution had no reasonable ground on which to refuse to disclose information.[43]

Some of the less controversial exceptions include mandatory non-disclosure of information:[44]

(i) Obtained in confidence from another government or international organization;[45]

(ii) Relating to third parties, where disclosure of such information is prohibited under section 8 of the Act.[45a]

Discretionary non-disclosure is permitted of information:

(i) Prepared by an investigative body for the purpose of determining whether or not to grant a security clearance;[46]

(ii) Prepared for sentencing purposes by the Canadian Penitentiary Service or National Parole Service or Board;[47]

(iii) That could reasonably be expected to threaten the safety of individuals;[48]

(iv) Relating to a third party;[49]

(v) Subject to solicitor-client privilege;[50]

(vi) Relating to the health of the applicant, when provision of that information would be contrary to the best interests of the individual.[51]

However, again the most wide-ranging and draconian of any exceptions relate to international affairs, defence and law enforcement.[52] These are the areas where the civil liberties of individuals are under threat. Government institutions operating in these areas have the capacity and, as we have shown,[53] the legal power to gather much personal information about an individual. If access to information is unduly restricted, the individual is left uncertain as to precisely what information is being gathered and the manner in which government institutions are operating. This, we have seen, has occurred in relation to the law enforcement agencies in Canada.[54] We have argued previously that a direct consequence of such powerlessness on the part of the individual, is the inhibition of his rights.

Pursuant to section 21, non-disclosure is permitted if the requested information:

> could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada, or any state, allied or associated with Canada, towards detecting, preventing, or suppressing subversive or hostile activities ... including and without restricting the foregoing, any such information listed in paragraphs 15(1)(a)-(1) of the Access to Information Act.

Section 21 is couched in wide terms and significantly restricts the disclosure of information. As Rankin observes, it contains a broad harms test followed by an equally broad class test justifying non-disclosure.[55]

The vagueness inherent in section 21 allows the head of government institutions further scope to refuse disclosure. First, the harms test used in section 21 is vague.[56] There is no indication of the amount of harm that is necessary to constitute an injury to the conduct of international affairs etc.[57] Such a test facilitates non-disclosure by the head of a government institution, who will have an inherent bias towards government efficiency and consequently non-disclosure.[58] The Act fails to recognize this, as in cases involving section 21 there is only limited judicial review. Pursuant to section 49 of the Act, a court will only order non-disclosure if it determines that the head of the institution had no reasonable grounds to justify non-disclosure.[59]

A second area of uncertainty in interpreting section 21 concerns the classes of exceptions listed in subparagraphs (a)-(i) of section 15 of the Access to Information Act. In particular, are these categories merely examples of conduct injurious to the nation, or do they represent separate and additional classes of exceptions.[60] It is submitted that they are merely examples. Both section 21 of the Privacy Act and section 15(2) of the Access to Information Act, after referring to the harms test, states "without limiting the foregoing any such information" and then lists the categories (a)-(i). The words "such information" can only refer to the information that was discussed earlier in the section, that is information injurious to international affairs, defence, etc.

Disclosure of information can also be denied pursuant to section 22 of the Act on the ground that it was obtained or prepared by an investigatory body[61] in the course of lawful investigation pertaining to:

(i) The detection, prevention or suppression of crime;[62] or

(ii) The enforcement of any law of Canada or a Province;[63] or

(iii) In circumstances where disclosure of information could reasonably be expected to be injurious to the enforcement of any law of Canada or of a Province or the conduct of lawful investigation.[64]

The actual terminology employed in section 22(1)(a) is very broad. The words "detection, prevention or suppression of crime" in subparagraph (i) cover all aspects of the criminal process. The phrase "enforcement of any law of Canada or a Province" used in both subsections 22(1)(a)(ii) and 22(i)(b), it is submitted, includes not only statute law but also includes regulations and the common law.

The court in Re Ontario Film and Video Appreciation Society & Ontario Bd of Censors,[65] held in a decision concerning section 1 of the Charter that the "'essence of law' was some form of legal force as distinct from administrative directions". Therefore, it included regulations and common law. The same logic could apply equally to subsections 22(1)(a)(ii) and 22(1)(b) of the

Privacy Act. Section 22(3) of the Privacy Act further supports this conclusion by its use of the phrase "investigations pertaining to the administration or enforcement of any Act of Parliament". The Act specifically refers to an "Act of Parliament" when a limitation of the meaning of "law" is intended. As it has not imposed such a restriction in section 22(1), the broader interpretation of "law" should be adopted.

Furthermore, the vagueness inherent in section 22 increases the likelihood of its wide use by government institutions. Section 22(1)(a) imposes the test of whether the information "pertains" to the detection of crime or enforcement of law. There is no guide as to how close the relationship must be between the information and the detection of crime or law enforcement.

### (iv) Summary of Effect of Exemptions to the Right of Access

The net effect of the various exemptions to the Act and exceptions to disclosure is a serious erosion of the principle that the individual has a right to access to personal information in government databanks. Some commentators have suggested that it amounts to a licence to withhold information.[67] Again, it is in the area of law enforcement and intelligence operation that the Privacy Act has the least impact.

The approach taken by the Privacy Act to the principle of access to information represents a compromise between the regulatory and self-regulatory approach.[68] There is an element of regulation in that in certain circumstances there is judicial review of the decisions of the head of a government institution refusing disclosure of personal information. However, there is no interference in the actual mechanics of access to information. The Act requires an application by an individual before the question of access can be considered.

Informational technology however, has shielded government institutions from scrutiny.[69] Therefore, individuals will be unaware of the circumstances in which they should exercise their right to request information.

It is submitted that what is required is for the Privacy Act to be amended to facilitate greater use of access rights. This would adopt a more regulatory model to the question of access to information. It is suggested that the head of a government institution be required, in specific circumstances, to notify the individual about the disclosure or use of the information by the institution. In particular, the individual should be notified when information is disclosed by a government institution under section 8(2) of the Act, or where the government institution uses information in relation to a decision concerning the employment, or the withholding of a license or benefit to the individual. Notification could take the form of identifying the nature of the information used or disclosed by the institution. Exceptions to notification could be made in the circumstances set out in sections 19-28 of the Act.

An expanded right of access would assist the individual in becoming aware of the informational practices of government institutions and, therefore, assist the individual in determining whether information is being handled fairly by government institutions.

## (b) Standards in Handling Personal Information

Sections 4-8 of the Privacy Act create standards to be observed by government institutions when handling information. The ability of these standards to instill in the individual a belief in the fair handling of information will depend on two issues:

(i) Are the enacted standards sufficiently strict;

(ii) Is the observance of the standards by government officials adequately enforced.

### (i) The Enacted Standards

Sections 4 and 5 of the Act deal with the collection of information.[78] Under section 4, no personal information is to be collected by a government institution "unless it relates directly to an operating program or activity of the institution". Section 5 requires personal information to be collected "wherever possible directly from the individual to whom it relates". Exceptions are created in subsection 5(3) where compliance with this directive would result in inaccurate information being collected or would defeat the purpose or prejudice the use for which the information was collected.

Although sections 4 and 5 are clearly desirable, in some respects they are too narrow. There is no requirement on the government institution to take steps to ensure that the information being collected is accurate, up-to-date or necessary for an operating program of the institution.[71] The danger is that too much information can legally be collected by government institutions. Further, there is no equivalent to the provisions in the Australian Privacy Act which require, in certain circumstances, the collector of personal information to take reasonable steps not to intrude to an unreasonable extent upon the affairs of the individual concerned.[72]

Section 6 of the Privacy Act deals with the second stage of the informational process, namely the maintenance of information. It requires, (in conjunction with Regulation 4 of the Privacy Regulations[73]), that personal information be retained for a period of at least 2 years following the date of collection. Further, subsection 6(2) requires the government institution to take all reasonable steps to ensure that the personal information used by the institution for an administrative purpose is accurate, up-to-date and complete as possible. Lastly, subsection 6(3) requires disposal of personal information in accordance with the Privacy Regulations. The only regulation dealing with disposal is Regulation 7, which requires there be no disposal for at least two years following disclosure of the information by the institution pursuant to subsection 8(2) of the Act.

Section 6 omits to regulate several important issues involving the maintenance of information. First, it does not impose a requirement that the information held should be adequate, relevant and not excessive (as appears in the U.K. Data Protection Act[74]). Such a requirement would restrict the amount of information being held by government institutions, which is one of the primary concerns of individuals with respect to the informational process.[75] Secondly, the requirements imposed by subsection 6(2) only apply to personal information used by the institution for an administrative purpose. "Administrative purpose" is defined in section 3 of the Act as relating to a decision-making process that directly affects the individual. It therefore does not apply to information that is simply held by a government institution and not used by it, or even information disclosed by the institution. In both of these cases, there is no administrative purpose, and therefore no requirement to observe the standards set out in subsection 6(2). Lastly, requirements regarding disposal of information need to be enunciated. Otherwise, the spectre of being traced from the "cradle to the grave"[76] becomes more of a reality. Again, by way of comparison, the Data Protection Act (U.K.) imposes a requirement that information shall not be kept for longer than is necessary for the particular purpose.[77]

Use of personal information is restricted by section 7 of the Act, which states that personal information can only be used by the institution:

(i) For the purpose for which it was obtained; or

(ii) For a purpose for which the information may be disclosed under subsection 8(2).

While it is desirable to impose such confidentiality-type requirements, there may be an anomoly which undermines the effectiveness of section 7. Under section 7 disclosure of information is permitted for a purpose for which the information may be disclosed under subsection 8(2). However, subsection 8(2)(m) includes a very broad exception permitting disclosure of information:

> for any purpose where in the opinion of the head of the institution,
>
> (1) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure.

In the context of section 8, this exception to disclosure is intended to be used sparingly. Section 8(5) requires the Privacy Commissioner to receive notification from the head of the institution on each occasion of non-disclosure under this subsection. However, section 7 does not refer to subsection 8(5) (which by its wording only applies to disclosure of information under subsection 8(2)). Therefore, arguably there is no such limitation concerning the use of information under section 7. The effect is that the information may be able to be used in any case where the head of the institution is of the opinion that the interest in disclosure clearly outweighs any invasion of privacy.

Lastly, section 8 attempts to regulate disclosure of information by government institutions. There are thirteen listed classes authorizing the disclosure of information which can conveniently be divided into two categories.[78] First, information that may be disclosed to certain designated institutions. Relatively non-contentious institutions including Attorney-General of Canada for use in legal proceedings,[79] Members of Parliament for assisting individual resolve a problem,[80] Public Archives for archival purposes,[81] persons for research,[82] associations of indigenous people in relation to grievances of their people,[83] government institutions for collecting debts,[84] and officers or employees of institutions for internal audit.[85]

However, subsection 8(2)(e) is far more

contentious. It permits information to be disclosed to an investigative body for the purpose of law enforcement upon written request of the law enforcement agencies. The designated investigative bodies are set out in Schedule II of the Privacy Regulations and include most of the law enforcement agencies in Canada. We have already shown that the area of law enforcement is one of special concern to civil liberties. Subsection 8(2)(e) simply ignores these concerns and allows law enforcement agencies to acquire information from other government institutions with little restriction.[86]

Secondly, information may also be disclosed under three broad purpose clauses.[87] These include disclosure of information for the purpose for which it was obtained or a use consistent with that purpose[88] and disclosure where authorized by an Act or Regulation.[89] The third purpose clause is far wider.[90] Subsection 8(2)(m), discussed previously, allows disclosure where, in the opinion of the head of the government institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from non-disclosure. Subsection 8(5) does require that the Privacy Commissioner be notified, if possible in advance, when the head of a government institution intends to disclose information in accordance with subsection 8(2)(m). The Privacy Commissioner may in turn notify the individual concerned.[91]

A provision such as subsection 8(2)(m) is clearly putting the efficiency of the government institution ahead of the intrusion into the personal life of the individual. It is difficult to see how an individual can be satisfied of government informational practices, when such a discretion resides with the head of the institution to disclose information.

### (ii) Enforcement of Sections 4-8 of the Privacy Act

A major limitation on the effectiveness of sections 4-8 lies in its lack of an effective mechanism to ensure observance of the enacted standards. There is no judicial review in respect of alleged infringements of the standards by government institutions.[92]

The only available remedy is an investigation by the Privacy Commissioner. Such an investigation may be initiated by a complaint by an individual.[93] Alternatively, the Privacy Commissioner, pursuant to s37 of the Act may from time to time carry out investigations of government institutions to ensure their compliance with sections 4-8.

The relief afforded by an investigation by the Privacy Commissioner is limited. The Privacy Commissioner only has the power to make recommendations and report abuses to the head of the particular institution,[94] or include the matter in his annual, or special report to the Parliament.[95] There are no coercive powers available to the Privacy Commissioner. The penalty for non-compliance by an institution lies only in the political process. In practical terms, it is difficult to see the Privacy Commissioner having the resources to undertake a comprehensive audit of the files and practices of government institutions.

This lack of enforceability is a serious deficiency in the Act. As we have seen, informational technology has provided government institutions with the ability to provide a better service.[96] It follows that officials of government institutions will have a bias towards utilizing such technology. After all, the benefits of such utilization are readily apparent and the standards by which their performance is assessed.[97] Therefore, in the absence of external scrutiny, it is impossible for the individual to form a belief (justified or not) that the individual has overcome this bias and is voluntarily complying with the inherently vague standards set out in sections 4-8.

In addition to this fundamental objection, the language used in sections 4-8 is not likely to influence government officials to voluntarily comply with the standards enacted.[98]

By necessity, sections 4-8 uses broad and imprecise language. Section 4 refers to information relating directly to an operating program or activity of the institution. Section 5 is even wider and requires the government official "wherever possible" to obtain information directly from the individual to whom it relates. Section 6 requires that reasonable steps be taken to ensure that the information used for an administrative purpose is accurate, up-to-date and complete.

Words such as "wherever possible", "reasonable" and "directly related to an operating program" call for a subjective interpretation by the particular government official. As such, where there is no external scrutiny, they are unlikely to alter an official's use of information.

Section 8 of the Privacy Act may be slightly more effective in influencing the behaviour of government officials in relation to the disclosure of information. At least compliance with the section can be ascertained from an objective viewpoint (i.e. did the disclosure fall within one of the listed categories). Further, in respect of information disclosed pursuant to subsection 8(2)(e), a record of the information disclosed must be kept for not less than two years,[99] therefore permitting the possibility of future scrutiny. However, subsection 8(2)(a) does allow disclosure for a purpose consistent with the purpose for which the information was collected. Again, this requires a subjective opinion of such purposes by the government official.

### (c) Indexing of Information Banks of Federal Government Institutions

In the context of the protection of civil liberties from advances in informational technology, the indexing of databanks, as provided by section 11 of the Act is obviously of limited significance. It does, however, accomplish three useful purposes.

First, it ensures that there are no databanks whose very existence is secret.[100] Secret databanks would create a serious threat to civil liberties. The anonymity of government institutions would be enhanced, and the individual would be left powerless to confront any abuses by such institutions.

Secondly, the indexing of databanks facilitates access by individuals to their personal information.[101] Section 11(1)(a)(iv) requires the index to include a statement of purposes for which information is held in the banks. When information is used by a government institution for some other purpose, the purposes set out in section 11(1)(a)(iv) must be modified to include the additional purpose. Through the statement of purposes, the individual can form some idea as to what information is likely to be held by a particular government institution.

Thirdly, the index provides for some accountability of government institution in respect of the information which they collect and hold. The statement of purposes will assist in ascertaining if a particular institution is going beyond its legal powers to obtain information.

### (d) Right of Privacy Under the Privacy Act

The Privacy Act does not define the term "privacy". Instead, section 2 sets out the purpose of the Act which is:

> to extend the present laws of Canada, that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to such information.

The conceptual basis of privacy in the Act is ambiguous. It appears clear that the Act does not regard privacy as a right. It does not define it anywhere or ever set out its terms. Further, section 2 makes reference to the "right of access", whereas no such inference is made in the section to the right of privacy (i.e. presumably not regarding the latter as a right).

Some assistance is gained from section 8(2)(m), which is the only other place in the Act where reference is made to the term "privacy". Subsection 8(2)(m) refers to the "invasion of privacy that could result from non-disclosure". This subsection seems to imply that privacy is a state, which can be invaded by the actions of government institutions. As such, it may give rise to a right (as in the case of the individual's right of access to personal information).

In considering whether the approach adopted in the Privacy Act is correct, the first question that we should address is what are the differences, in practical terms, if a right of privacy was created. The differences are fourfold.

First, a purpose clause, as provided in section 2, will assist a liberal construction of a section in the Act where some ambiguity exists.[102] Therefore, the interpretation that respects privacy should be adopetd. What a purpose clause cannot do is to fill in omissions or assist where there is no ambiguity.[103] As stated by Muirhead J in *Lindner* v *Wright*,[104] "I must of course regard it as settled law that it is no power of the judicial function to fill gaps disclosed in legislation". A right of privacy can go further than merely assisting where there is ambiguity. Application of the principle generalia specialibus non derogant,[105] would ensure that a general right of privacy would not prevail over some other specific right. However, where the specific section does not refer to a particular situation, the general right can operate. For example, a right of privacy might prevent collection of information from a source which had been supplied with confidential information by an individual. This might well infringe a right of privacy, whereas section 2 could not assist as there was no ambiguity.

Secondly, a right of privacy would reverse the onus of proof. It would be up to the government institution to justify the infringement of the right. At present, the individual has to prove all elements of the infringement.

Thirdly, a right of privacy, even if subject to various limitations, would play some role in influencing the behaviour of government officials when handling information.[106] That is, the right of privacy possesses normative influence beyond that which a mere catalogue of rights might produce.[107] Government officials must consider the right of privacy of the individual before taking a particular cause of action. As Dworkin says:

> if rights make any sense at all then the invasion of a relatively important right must be a very serious matter. It means treating a man as less than a man or less worthy of concern than other men.[108]

A responsible government official, even if he decides to infringe the individual's right of privacy, will only do so after due consideration of the limits of the applicability of the right or by assigning some other right greater value.[109] The bias of the government official in favour of the efficiency of the government institution will still exist, and will diminish the influence of this aspect of the right of privacy. Nevertheless, the reasons we have stated clearly enunciated a right is likely to have more influence on the behaviour of government officials than the vague, unenforceable duty imposed by sections 4-8 of the Act.

Fourthly, we have argued in this paper that the individual's beliefs in the fair handling of information by government institutions is critical to the individual's civil liberties. A right of privacy would assist the formation of this belief by giving the individual legal control over information. The legal right to control information (being an aspect of the right of privacy), can thus be used to establish the extent of the liberty to be enjoyed by the individual. As Fried says:

> Legal rules play a large part in establishing the societal context of privacy. These rules guarantee to a person the claim to control certain areas, his home, perhaps his telephone communications and back this guarantee with enforceable sanctions. What is less obvious is that the law is not just an instrument for protecting privacy; it is an essential element in our culture of the institution itself. The concept of privacy requires, as we have seen, a sense of control and a justified acknowledged power to control aspects of one's environment. But in most developed societies the only way to give a person the full measure of both the sense and fact of control is to give him a legal title to control.[118]

The preceding discussion is not intended to simplify the considerable intellectual debate over the nature of privacy, and in particular whether it is properly classified as a right, on a principle or a state.[111] What it is intended to illustrate is that, in the context of the Privacy Act, a right of privacy in the informational sense would be a very useful tool to employ.

The next issue is whether a practical wording definition of privacy can be found for the purposes of the Privacy Act. Again, there exists considerable academic uncertainty as to whether a unitary definition of privacy is possible.[112] For example, the Younger Committee on Privacy in the United Kingdom found that "there was no satisfactory definition that could be used for the purpose of enacting a general law of privacy and that no such law was needed."[113] The Committee concluded that the notion of a right of privacy was confusing and that specific rights should be enumerated and defined.

However, in the context of the Privacy Act, we are only concerned with a right of informational privacy and, therefore, do not have to consider how this right fits in with other aspects of privacy.[114] The Younger Committee did not disagree with this approach and singled out the right of informational privacy as one that needed to be expanded.[115]

The leading definition of informational privacy is

Westin's, who defines privacy as:

> the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.[116]

The Ontario Commission on Freedom of Information, Privacy and Computers,[117] the Report of the Task Force established by the Department of Communications/Department of Justice,[118] and the Supreme Court of Canada in R v Dyment,[119] have all adopted this definition.

Westin's definition has been criticized, but mainly in the context of its use in providing a comprehensive definition to all aspects of privacy. Greenwalt gives the example of a brainwashed or raped person, who has suffered an extreme loss of privacy, but not necessarily any loss of control over information.[120] Schaeffer gives a similar example of a University professor suffering from various disturbances, whilst trying to work.[121] Issues involving personal choice, such as abortion, are also excluded.[122] These criticisms however, are irrelevant if we restrict the definition to its informational context.

Some commentators have suggested that, even if restricted to the informational context, Westin's definition is too broad. O'Brien gives the example of a person who gains information about another by simple observation.[123] In such a case, the observed person has lost control over personal information, but in many instances, it would be too trivial to class as a loss of privacy.[124] In other words, the definition sets too low a threshold before the right of privacy is infringed.

It is submitted that these criticisms can be overcome in the context of the Privacy Act by declaring a general right of privacy in accordance with Westin's definition, but then providing that a government institution shall be deemed not to have infringed such a right, if it acts in accordance with the informational privacy principles. These principles, as sections 4-8 of the Act do now, would provide restrictions on the ability of government institutions to collect, hold and disclose information. Therefore, in cases such as the one outlined by O'Brien, there would be no infringement of the informational principles and therefore no infringement of the right of privacy. Both the Privacy Act of Australia[125] and the Data Protection Act of the U.K.,[126] use the informational privacy principles to determine how government institutions should handle information, though neither Act uses them in conjunction with an express right of privacy.

Such an approach, as we shall see later, would also allow for a consistent approach with any right of privacy that might be declared under section 7 of the Charter. In particular, the informational privacy principles could be employed in determining, in the privacy context, whether a deprivation of liberty was in accordance with the principles of fundamental justice.

### (3) Conclusion

The Privacy Act is clearly a welcome piece of legislation insofar as it attempts to control the informational process of government institutions. However, the preceding analysis has shown that the Act is not sufficiently sensitive to the civil liberties concerns of the individual. In particular, the Act is incapable of satisfying the individual that government institutions are handling personal information fairly for the following reasons. First, the Act only applies to federal government institutions and not provincial government institutions. Secondly, the only explicit right given to the individual in the Act is a right of access to information. There is no right of privacy, which might give the individual legal control over information. Even the right of access is weakened by many broad restrictions justifying non-disclosure of information by government institutions. Thirdly, the standards enacted in sections 4-8 of the Act are too narrow in some respects and suffer from a lack of enforceability.

## PART 3. ACCESS TO INFORMATION ACT

The Access to Information Act[127] is the companion

Act to the Privacy Act. It is virtually in identical terms, and the previous analysis of the Privacy Act, its rights of access, exceptions and exemptions, is directly relevant. The Access to Information Act also requires details of the type of information held by government institutions to be published on an annual basis,[128] but contains no provisions corresponding to sections 4-8 of the Privacy Act regulating the informational process.

The essential difference between the Acts is that the Privacy Act is intended to provide access and regulation of personal information, while the Access to Information Act is intended to provide access to public information.[129] Section 2 of the Act states:

> that the purpose of the Act is to extend the laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public.

"Records" is defined broadly to include virtually any form of reproduction of information, including computerized information, and even information that can be created by the application of normal computer technology.[130]

The same system of refusal of access is provided by the Access to Information Act as the Privacy Act. Section 4 of the Access to Information Act gives the individual, subject to other provisions of the Act, a right, upon request, to access to records held by a government institution. Again, the Act does not apply to cabinet records which have been in existence for less than 20 years. The head of the government institution may also refuse disclosure on the same broad exceptions as contained in the Privacy Act.[131]

The procedure for reviewal of a refusal of access is the same as the Privacy Act. The individual initiates a complaint to the Information Commissioner under section 30 of the Act. The Information Commissioner investigates the complaint and makes non-binding recommendations.[132] Either the individual[133] or the Informational Commissioner on his behalf[134] may apply to the Federal Court if refusal to disclose is maintained by the head of the government institution. The Federal Court may order disclosure if it finds that the head of the institution was not authorized to refuse disclosure[135] or, in certain cases (including cases involving defence, international affairs or law enforcement), upon the strictest test that the head of the institution had no reasonable grounds to refuse disclosure.[136]

The importance of the Access to Information Act is that it assists in ensuring the accountability of government institutions. Individuals are given the information necessary to challenge and debate government decisions.[137] It is therefore more difficult for government institutions to conceal abuses. For example, in the United States, illegal activities of the C.I.A. and F.B.I. became known through that country's Freedom of Information Act.[138]

The effect on civil liberties is two-fold. First, the possibility of abuses being discovered (such as in the cases of the F.B.I. and C.I.A. or even the R.C.M.P.)[138] will influence government officials not to engage in illegal activities that threaten civil liberties. Secondly, lack of accountability of government institutions is one of the factors that have led individuals being rendered powerless by advances in informational technology.[139] A consequence of this powerlessness has been an unwillingness on the part of the individual to exercise its liberties.

However, as with the Privacy Act, the broad exemptions to the right of access has seriously eroded the effectiveness of the Act. In particular, accountability in areas such as law enforcement or defence has not been greatly enhanced.

## PART 4. THE CRIMINAL CODE

### (1) Introduction

Part VI of the Criminal Code,[140] which reproduces the Protection of Privacy Act,[141] is headed "Invasion of

Privacy". It does not, as the name might imply, introduce a comprehensive scheme for the protection of privacy.[142] Rather, it attempts only to regulate electronic interception of private communications. The Code, therefore, has relevance to only one aspect of the informational process, namely the ability of government institutions to acquire information about individuals. Even in this area, the impact of the Code is reduced by the advances in technology which, as described in Chapter II, have enable government institutions to acquire information from various sources without requiring any direct surveillance.

Advances in technology have increased the capacity of law enforcement agencies to undertake electronic surveillance.[143] We have referred previously to miniaturization of listening devices and parabolic microphones,[144] but in the area of electronic surveillance, technology is even more sophisticated with laser beams and electronic ways capable of intercepting communication in a room when aimed at a wall or window[145] and combination mirrors, which can transmit both sight and sound.[146]

The circumstances in which electronic surveillance is permitted by government institutions in a liberal democracy is of considerable importance to civil liberties. Electronic surveillance is one of the most pervasive and indiscriminate forms of surveillance.[147] It is indiscriminate in the sense that it affects not only the particular subject, but all persons with whom those subjects come into contact, or even all persons in a particular area.

The danger to civil liberties from electronic interception of communications is two-fold. First, there is the obvious intrusion into the individual's personal life through such surveillance. Secondly, there is the danger that such a comprehensive form of surveillance will cause the general public to refrain from exercising their liberties.[148] As we discussed previously, the very act of surveillance can cause an individual to be inhibited or, in the extreme, redefine his activity as illegal.[149] To prevent this from occurring, there is the obvious need for the individual to be reassured that electronic surveillance is controlled and permitted only in limited circumstances.[150]

Government institutions, and in particular law enforcement agencies, view the use of electronic surveillance very differently. Electronic surveillance enables such bodies to obtain information not otherwise available. They claim, therefore, that electronic surveillance is an essential part of their crime fighting armory, especially in the area of organized crime.[151]

Part VI of the Code attempts to balance these two conflicting goals.[152] As Craig says:

> sooner or later there will be no limit to the degree of surveillance possible.[153]

That is, previous physical barriers will become irrelevant. It is submitted however, that although introducing some positive measures, Part VI does not satisfactorily achieve this balance between government efficiency and civil liberties. It allows for considerable government intrusion into the personal life of individuals by permitting electronic surveillance in many circumstances. Rather than restricting, it threatens to permit proliferation of wiretapping.[154]

**(2) Operation of the Act**

Part VI of the Code seeks to regulate electronic surveillance by rendering it unlawful unless authorized by a judicial warrant.

Under section 184 of the Code, it is an indictable offence to intercept private communications by electronic surveillance. Section 183 defines private communications as:

> any oral communication or any telecommunication made under circumstances where it is reasonabl for the originator to expect that it will not be intercepted by any person other than the person intended by the originator thereof to receive it.

This section has been broadly interpreted. In

Goldman v The Queen,[155] the Supreme Court of Canada considered that the "originator" of communications for the purpose of this definition was the person who makes the statement which the Crown later seeks to use.[156] The court gave two reasons for coming to this decision: first the purpose of the Act was to protect privacy, and therefore a liberal construction should be adopted; secondly, the nature of a "communication" involved the passing of ideas from one person to another. Therefore, who actually initiated the conversation was irrelevant. Cases involving undercover agents will therefore come within the Act,[157] though it will still be necessary for the individual to establish that he had a reasonable expectation that the conversation would not be intercepted.[158]

Section 184 will not apply where:

(i) One of the parties has consented to the interception;

(ii) The interception has been made pursuant to judicial authorization;

(iii) The interception was made in specified circumstances by an employee of a telephone or like company;

(iv) The interception was made by federal government employees monitoring radio frequencies.[159]

Obviously, the major thrust of the Act concerns authorization by judicial warrant. However, the consent exception also errs in favour of law enforcement agencies. Because section 184(2) requires consent of either the originator of the communication, or the intended recipient, it has been held that a consent given by a police informant is valid, thereby rendering the interception legal.[160]

It is difficult to see why such a situation should not require a warrant. Intrusive and possibly irrelevant material is being gathered by the informer. Further, the enforcement agency is aware in advance of the possibility of gaining evidence, hence the interception of communications.

## (3) Judicial Warrant System

### (a) Introduction

The introduction of the judicial warrant system is a positive innovation, although experience has suggested that the vast majority of warrant applications will be granted.[161] It is suggested that any problem of judicial "rubber-stamping" of warrant applications is not inherent in the system of judicial warrants, but results from lack of sufficient information to make an independent assessment. Once provided with sufficient information, a judge, being accustomed to balancing competing interests, is likely to duly calculate the importance of protection to an individual's liberty.[162]

Furthermore, a judicial warrant system helps ensure future accountability by providing a record of the grounds put forward in support of an application.[163] Under a judicial system a great deal of information is kept, including evidence of compliance with the safeguards expressed in the Code. The Code also requires the Solicitor-General of Canada and the Attorney-Generals of the Provinces to prepare an annual report to be presented to Parliament, giving details of the warrant applications.[164]

Government officials requesting a warrant are made aware that there is a permanent record of their claimed need to undertake surveillance, and may therefore be influenced not to abuse these powers, whether through fear of legal action being taken against them (a remote possibility), or through concern at the risk of public exposure and further restraint on their powers.[165]

Furthermore, the warrant provides a procedural alert for government officials - it alerts them to the need to justify surveillance. In framing an application in accordance with the procedures required under the Code, and in expressing reasons for the surveillance, the officer may review the need for surveillance.[166]

(b) Authorization of Warrants

Part VI of the Criminal Code fails, not in its implementation of a judicial warrant system, but because of its wide authorization of warrants and lack of procedural safeguards.

Electronic surveillance may be authorized in respect of the offences specified in section 183(a), or in respect of an investigation of offences under the Criminal Code, where the presribed penalty is not more than five years imprisonment, or where there are reasonable and probable grounds to believe that the target of surveillance is part of a criminal activity, planned and organized by a number of persons acting in concert.[167] Such a broad provision is unnecessary. As various commentators have observed, there are fifty seven offences falling within this category, including petty theft, impaired driving, etc.[168]

The risk to civil liberties occasioned by such a broad provision is three-fold. First, there is the obvious intrusion upon the subject of the surveillance. Secondly, there is the danger that private information about innocent third parties is recorded. Thirdly, there is the public perception of widespread police surveillance and the consequent chilling of an individual's behaviour and speech.

The procedure in applying for a warrant also pays insufficient attention to the individual. Under section 185 of the Code, an application is made ex parte upon the affidavit of the Attorney-General of a Province or by the Solicitor-General of the designated agent.[169] The application must be accompanied by an affidavit setting out the facts relied upon to justify surveillance, including details of the offence,[170] the type of communications proposed to be intercepted,[171] the type of communications proposed to be intercepted,[172] the persons whose private communications it is reasonably probable will be intercepted,[173] and previous instances of surveillance over the same persons named.[174]

The judge may grant the authorization if satisfied that it is in the best interests of the administration of justice to do so, and that other investigative procedures have tried and failed or are unlikely to succeed or are impractical.[175] The warrant is valid for 60 days, unless extended.[175a]

This application procedure can be criticized on two broad grounds. First, the application is made in secret, hidden from external scrutiny. This creates the possibility of abuses by law enforcement agencies. For example, the McDonald Commission found that such agencies would "forum shop" amongst judges, until they gained authorization.[176] Further, the application and supporting evidence are placed in a sealed package and remain confidential.[177] As Deutscher observes, this makes it difficult to test the standards employed by the law enforcement agency or by the judge to whom the application is made.[178] There is a provision in the Code for the sealed package to be opened upon application to a judge of a superior court.[179] Prior to the enactment of the Charter, this would only be done in circumstances where the subject of the surveillance had been charged and there was extrinsic evidence of fraud in obtaining the warrant.[180] However, section 8 of the Charter has been interpreted as requiring that the accused be given a right of access to the sealed package, irrespective of proof of fraud, if such access is required for the defence.[181] R v Kumar[182] made it clear that such access to the sealed package did not apply where the accused had not been charged.

Secondly, it is submitted that the application procedures do not supply the judge with sufficient information to make an informed decision on the granting of a warrant. All the evidence is supplied by the law enforcement officer by affidavit. There is no opposing evidence called, or even cross examination upon the evidence produced. In such cases, law enforcement officers with a natural bias towards the efficient workings of their department and an asserted need for surveillance in the application, are unlikely to be sensitive to civil liberties. It is more likely, therefore, that a judge would form the view that the authorization was in the best interests of justice, and that alternative methods of investigation are not possible.

It is suggested that the recommendations of the British Royal Commission on Criminal Procedure be adopted and that the interests of the subject of the surveillance be represented at the _authorization hearing of the official solicitor or a similar body.[183] If this proposal was adopted, the assertations of the law enforcement agencies could be better tested.

## (4) Safeguards

The Criminal Code also fails to provide adequate safeguards once an application has been granted. Pursuant to section 186(4), the authorization granting the warrant is requested to specify various terms and conditions. However, it is submitted that these terms and conditions fails to adequately protect the civil liberties of the individual.

Most objectionable is subsection 186(4)(e), which allows a warrant to be valid for a period not exceeding 60 days (the Protection of Privacy Act originally allowed a maximum period of 30 days, but the 1977 amendment to that Act increased the period to 60 days).[184] A 60 day time period is inconsistent with the particularity requirement in determining whether or not to grant a warrant. The risk is that the warrant becomes an extensive "fishing exercise".

Also objectionable is section 186(4)(c), which requires the authorization to:

> state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be given and generally describe the manner of interception that may be used.

It is not surprising that such a vague section has permitted a broad description of both persons and places in a warrant. For example, in R v Thompson et al,[185] it was held that an authorization permitting interceptions at certain premises and "elsewhere in the Province of British Columbia" was valid. Similarly, in R v Samson,[186] it was held that unknown persons can be specified in the authorization, although they should be identified by class.[187]

Section 186(3)(d) allows the judge to impose such terms and conditions as he considers advisable in the public interest. There have been no cases where an authorization has been held to be invalid for failure to impose such conditions. In R v Thomson,[188] the court held that the authorizing judge, when aware that the interception of communications was to be made at a public telephone, may be "wise" to impose some conditions protecting the privacy of innocent third parties. Also in R v Finlay and Grellette,[189] in considering the application of the Charter, the court held that subsection 4(d) should be used, when appropriate, to impose minimization requirements. It appears, therefore, that section 186(3)(d) gives the power, but does not impose any obligation on the part of the authorizing judge to impose terms and conditions in granting the warrant.

Part VI of the Code also includes the positive provision of requiring notification to the subject of surveillance.[190] The purpose of such a provision is two-fold. It grants the subject the opportunity to gather sufficient information to mount a civil suit against abuse by law enforcement agencies (a remote possibility). Also, it serves a warning on the government agency that unacceptable practices will be held accountable.

However, it is unlikely that these goals will be achieved.[191] Although section 196(1) requires notification to the subject within 90 days following the period of authorization, this may be extended, upon application of the Attorney-General, to a period not exceeding three years.[192] The judge granting the extension must be satisfied that the investigation is continuing (or a subsequent investigation using information derived from the interception) and that it is in the best interests of justice to grant the extension.[193] Again, in practical terms, this test leaves the judge with little discretion. If a law enforcement agency adduces evidence that a prosecution has not yet been laid and that the investigation has not been abandoned, it would be difficult for the judge, in the absence of the other party, to come to the conclusion that it was not in the best interests of justice to grant the extension. The danger with such a long period before notification, is that it makes it difficult for the individual to successfully challange the action of the law enforcement agencies. Witnesses may have moved or their recollection dimmed and the sense of injustice on the part of the subject of the surveillance may also have diminished with the passage of time.

Secondly, judicial interpretations of the notification provisions of the Act have also reduced their impact. In Re Zaduk and The Queen[194] it was held that a notification in the following terms was sufficient:

> This is to notify you that pursuant to s178-23 of the Criminal Code of Canada, that you have been the object of an interception pursuant to an authorization used under the Criminal Code."

As various commentators have observed, this notification gives the subject no information as to why or how he was under surveillance, thereby making it unlikely that a decision to undertake surveillance can be held accountable.[195]

Thirdly, as we have discussed, the sealed package within which the application and supporting material is placed, will not be opened where no charges are laid, in the absence of extrinsic evidence of fraud. The individual is thus provided with no means of ascertaining whether there has been misconduct on the part of law enforcement agencies.

## (5) Enforcement Provisions

The enforcement provisions of the Act are, on the whole, unsatisfactory. The Act does criminalize both the interception of private communications with authorization, and also the disclosure, without consent, of information obtained from such interpretation.[196] However, the impact of this provision is lessened by the shortcomings of the Act, referred to previously, in particular the ease with which the authorization may be obtained. As in other areas of informational law, it is difficult to detect transgressions by government officials, especially given the general secrecy in which surveillance operations are carried out. Therefore, as a means of influencing the behaviour of government officials, the imposition of criminal liability will probably have little impact. There have been no cases to date where government officials have been convicted of such an offence.

Consequent upon conviction, the accused may be liable to pay punitive damages not exceeding $5,000.00.[197] Section 7(2) of the Crown Liability Act imposes a form of vicarious liability on the Federal government, although there is no corresponding provision in respect of the Provincial government.[198]

The provisions in the Code enabling the award of punitive damages will have little impact in influencing government officials to be sensitive to privacy concerns. First, any award of punitive damages is dependent on the conviction of an offence imposing criminal penalties on a particular government employee. Secondly, the award of punitive damage is discretionary. This seems inconsistent with the purpose of the provision - if a particular act by a government employee is regarded by the legislature as sufficiently serious to impose criminal liability, then punitive damage should follow automatically.

The Code does create civil remedies. Pursuant to section 7(2) of the Crown Liability Act,[199] the Crown is liable for all loss or damage caused by, or attributable to an unauthorized interception. A defence is available if the Crown can show that the interception was lawfully made.[200] This has ben interpreted to mean that authorization was obtained in accordance with the Code.[201]

Section 7(2) has attached little judicial or scholarly attention.[202] McDonald does make the point that, in view of the above-mentioned defence, the offence will only apply where law enforcement officials have failed to obtain authorization for the warrant.[203] The subject of the surveillance will suffer procedural difficulties in bringing an action, including obtaining access to the information held by government institutions and satisfying the burden of proof. In addition, there is no corresponding provision in Part VI of the Code concerning the civil liability of Crown officials. Therefore, provincial government officials will not be subject to civil remedies as the Crown Liabilities Act does not apply to them.[204]

The Crown, both federally and provincially, will be subject to vicarious liability for associated torts committed by its employees in effecting electronic surveillance.[205] In R v Davis,[206] the Manitoba Court of Appeal held that, although authorized to conduct surveillance, government officials could not break the laws of the land, and common law remedies for trespass, assault and negligence would be available if appropriate.

Provisions in the Code relating to the admissibility of evidence are also objectionable.[207] Pursuant to section 189 of the Code, evidence obtained from unlawful interceptions is inadmissible against that person unless the defect is only in the form of an irregularity. However, information acquired from an unauthorized interception (i.e. derived evidence) may be used unless it brings the administration of justice into disrepute.[208]

Therefore, in the case of derived evidence, the burden of proof is clearly on the defendant to show that the evidence should not be admitted.[209] Further, the defendant must first prove that the evidence was in fact derived evidence obtained from an unauthorized surveillance.

It is submitted that such a provision is unacceptable. The Act is designed to discourage certain actions of law enforcement agencies because of their threat to civil liberties. However, by admitting such evidence, the intrusion goes unpunished.[209] Statistics, from the annual report of the Solicitor-General and Attorney-General involving surveillance evidence, suggest that in 76.6% of such cases derived evidence was used, while in only 23.4% of cases was primary evidence used.[210] Further, in many cases government institutions will use information obtained from surveillance, but need not lead it directly in evidence.

### (6) Charter

Part VI of the Code will be subject to scrutiny for fairness according to the provisions of the Charter, in particular section 8. We will examine later in this paper the impact of section 8 in this area.

## (7) Conclusion

Part VI of the Code has introduced a number of significant reforms. The implementation of a judicial warrant system, notification provisions and imposition of criminal sanctions are all positive features. As Burns says, the legislation is of the highest social value to Canada, recognizing the role of privacy and the need for its protection.[210]

However, the Code is insufficiently sensitive to the liberties of individuals.[211] There is an imbalance between the conflicting aims of protecting individuals from intrusion on the one hand, and the efficiency of government institutions and the protection of the welfare of citizens through the administration of laws on the other. This imbalance is reflected in the vast range of offences for which electronic surveillance is permitted, the extended duration of surveillance, and the relaxed rules relating to the admissibility of evidence and notification of the fact of surveillance to the subject.

The Code thus fails to adequately access the degree to which individuals' civil liberties are at risk from law enforcement action. It does little to alter attitudes of officials of law enforcement agencies to the need for surveillance.[213] One must therefore reach the conclusion that in Part VI of the Code, civil liberties have again been subrogated to the interests of government institutions, and in particular the law enforcement agencies.

## FOOTNOTES - CHAPTER IV

1. S.C. 1980-81-82-83, c111, Sch. II.

2. Rankin "Privacy and Technology: A Canadian Perspective" (1984) 23 Alta. L.R. 323, 325.

3. S.C. 1980-81-82-83, c111, Sch.I.

4. R.S.C. 1985, cC-46 replacing the Protection of Privacy Act 1970, cC-34 as amended.

5. Rankin "The New Access to Information and Privacy Act: A Critical Annotation" (1983) 15 Ottawa LR 1, 8. See Privacy Act S.C. 1980-81-82-83, c111, Section 3.

5a. Standing Committee on Justice, Open and Shut: Enhancing the Right to Know and the Right to Privacy (Ottawa Queen's Printer, 1987), at 74 ff.

6. Rankin Ibid 9.

7. Ibid.

8. Privacy Act S.C. 1980-81-82-83, c111, Section 12(1) and Section 41.

9. Ibid Sections 4-8.

10. Ibid Section 11.

11. Ibid Section 2.

12. Kallner "Personal Data: The Open Access Approach" in O.E.C.D. Policy Issues in Data Protection, Vol. 10 Informatics Series, (1984) 59.

13. Supra at p20 ff.

14. See Rule, McAdam, Stearns and Uglow. The Politics of Privacy (1980).

15. See Privacy Act S.C. 1980-81-82-83, c111, Section 29.

16. Ibid Section 35.

17. Ibid Section 41.

18. Ibid Section 47.

19. Ibid Section 18(1).

20. Rankin, supra n2 at 337.

21. S.O.R./83-374 entitled "Exempt Personal Information Bank Order No.14 (R.C.M.P.)

22. Flaherty "Protecting Privacy in Police Information Systems" (1986) 36 U of T L.J. 116, 119 citing S.O.R. 83/376 (Exempt Personal Information Bank Order No. 14).

23. (1984) 10 D.L.R. (4th) 587.

24. This was discussed in Re Ternette and the Solicitor-General of Canada as being the alternative type of review (1984) 10 D.L.R. 587, 595.

25. Ibid 594.

26. The Oxford English Dictionary (2nd ed, 1989), Vol. 5 p527, n4.

27. (1984) 10 D.L.R. 587, 594.

28. Faust "National Security Information Disclosure

Under the FOIA: The Need for Effective Judicial Enforcement" (1984) 25 Boston College LR 611, 636.

29. S.C. 1980-81-82-83, c111, Section 36 "The Privacy Commissioner may, from time to time, carry out investigations of the files contained in personal information banks designated as exempt banks under section 18."

30. Ibid Section 70(1)(a)-(f).

31. Rankin, supra n5 at 26.

32. Rankin supra n5 at 33.

33. [1942] A.C. 624. For a general discussion of Crown Privilege see Hogg Constitutional Law of Canada (2nd ed., 1985), 224.

34. Hogg Ibid citing Conway v Rimmer [1968] A.C. 910 and Burmah Oil Co. v Bank of England [1980] A.C. 1090.

35. Hogg Ibid citing R v Snider [1954] S.C.R. 479 and Smallwood v Sparling [1982] 2 S.C.R. 686.

36. (1983) 43 O.R. (2nd) 161, 201.

37. (1982) 134 D.L.R. (3rd) 17.

38. Federal Court Act, R.S.C. 1970, c10 (2nd Supp) Section 41(2) "When a Minister of the Crown certifies to any court ... that the production ... of a document ... would be injurious to ... national security ... production shall be refused without any examination of the document by the Court."

39. See generally Mann Computer Technology and the Law in Canada (1987), 209.

40. Privacy Act S.C. 1980-81-82-83, c111, Section 35.

41. Ibid Section 41.

42. Ibid Section 48.

43. Ibid Section 49.

44. Mann supra n39 at 209-10.

45. Privacy Act S.C. 1980-81-82-83, c111, Section 19.

45a. Ibid Section 26.

46. Ibid Section 23.

47. Ibid Section 24.

48. Ibid Section 25.

49. Ibid Section 26.

50. Ibid Section 27.

51. Ibid Section 28.

52. Ibid Section 22.

53. Supra at p.31.

54. Supra at p.30 ff.

55. Rankin supra n5 at 16.

56. Ibid.

57. Rankin supra n5 at 13.

58. Faust supra n28 at 613.

59. Privacy Act 1980-81-82-83, c111, Section 49.

60. Rankin supra n5 at 33.

61. As defined in Privacy Regulations SOR/83-508, regulation 5.

62. Privacy Act S.C. 1980-81-82-83, c111, Section 22(1)(a)(i).

63. Ibid Section 22(1)(a)(ii).

64. Ibid Section 22(1)(b).

65. (1983) 5 D.L.R. (4th) 766.

67. Onyshko "Access to Personal Information: British and Canadian Legislature Approaches" (1989) 18 Man. L.J. 213, 245.

68. Rankin supra n2 at 335.

69. Supra at p.22.

70. See Mann supra n39 at 214.

71. cf. Privacy Act (Aust) 1988, Section 14 principles 1(5) and 3(c).

72. Ibid s14, principle 3(d).

73. SOR/DORS 83-508.

74. Data Protection Act (U.K.) 1984 c35, Sch.1, principle 4.

75. Supra at p.11.

76. Benn "Technology and Society" in Rowe (ed.) Privacy Computers and You (1972), 14.

77. Data Protection Act (U.K.) 1984, c35, Sch.1, principle 6.

78. See Rankin supra n5 at 21-22.

79. Privacy Act S.C. 1980-81-82-83, c111, Section 8(2)(d).

80. Ibid Section 8(2)(g).

81. Ibid Section 8(2)(i).

82. Ibid Section 8(2)(j).

83. Ibid Section 8(2)(k).

84. Ibid Section 8(2)(l).

85. Ibid Section 8(2)(h).

86. Rankin supra n5 at 17.

87. Ibid 22.

88. Privacy Act 1980-81-82-83, c111, Section 8(2)(a).

89. Ibid Section 8(2)(d).

90. Rankin supra n5 at 22.

91. Privacy Act 1980-81-82-83, c111, Section 8(5).

92. Rankin supra n2 at 339.

93. Privacy Act 1980-81-82-83, c111, Section 29.

94. Ibid Section 35.

95. Ibid Section 38 and Section 39.

96. Supra at p.1.

97. Ibid.

99. SOR/DORS 83-508, reg. 7.

100. See Kirby "National Forum on Access to Information and Privacy" (1986) 60 ALJ 317, 319.

101. Ibid.

102. Rankin supra n5 at 4.

103. See MacAdam & Smith Statutes, Rules and Examples (1985), 241.

104. (1976) 14 A.L.R. 105, 108-111.

105. See Maxwell The Interpretation of Statutes (10th ed., 1953), 176 for a discussion of this principle.

106. Burns "The Law and Privacy: The Canadian Experience" (1976) 54 Can B.R. 1, 7 citing an argument from Lusky.

107. See O'Brien Privacy Law and Public Policy (1979), 11; Bloustein "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1965) 39 N.Y.U.L.R. 962, 963.

108. Dworkin "Taking Rights Seriously" (1977), 199.

109. Ibid 93.

110. Fried "Privacy" (1968) 77 Yale LJ 475, 483.

111. eg. See O'Brien supra n 107, Bloustein supra n107, Gavison "Privacy and the Limits of Law" (1980) 89 Yale LJ 421; Mashall "The Right of Privacy: A Skeptical View" (1975) 21 McGill LJ 242. Schaffer "Privacy: A Philosophical Overview in Gibson" "Aspects of Privacy Law" (1980).

112. Ibid; see also Parker "A Definition of Privacy" (1974) 27 Rutgers LJ 275; Westin "Privacy and Freedom" (1967), 32 ff. Prosser "Privacy" (1960) 48 California LR 353.

113. Report of the Committee on Privacy, (The Younger Report) Cmnd 5012, (1972), 18, 22.

114. See Westin supra n112 at 32 ff. for a discussion of the various types of privacy. See La Forest J in R v Dyment (1989) 55 D.L.R. (4th) 503, 513, who accepts 3 aspects of privacy - territorial, personal and informational.

115. Report of the Committee on Privacy, Cmnd 5012, (1972), para.659.

116. Westin, supra n112 at 7.

117. Ontario Commission on Freedom of Information and Individual Privacy, Vol. 3, Protection of Privacy (1980).

118. Privacy and Computers, the Report of the Task Force established by the Department of Communications/Department of Justice (1972), 13.

119. (1989) 55 D.L.R. (4th) 503, 515.

120. Greenwalt "Privacy and Its Legal Protection" (1974) 2 Hastings Centre Studios No. 3 cited in Shattuck "Rights of Privacy" (1977), 198.

121. Schaeffer supra n111 at 7.

122. O'Brien supra n111 at 15.

123. Ibid 13.

124. Ibid.

125. Privacy Act (Aust) 1988, Section 14.

126. Data Protection Act (U.K.) 1984, c35, Section 2.

127. S.C. 1980-81-82-83, c111, Sch.1.

128. Ibid Section 5.

129. Ibid Section 2.

130. Ibid Section 3.

131. Ibid Sections 13-26.

132. Ibid Sections 30, 37.

133. Ibid Section 41.

134. Ibid Section 42.

135. Ibid Section 49.

136. Ibid Section 50.

137. Acces a L'Information et Protection Renseignements Personelle (ed. 1984) 400.

138. Ibid 403.

139. Supra at p.20 ff.

140. R.S.C. 1985, cC-46, Section 1.

141. S.C. 1973-4, c50. Amend S.C. 1976-77, c53.

142. Burns "A Retrospective View of the Protection of Privacy Act: A Fragile Rede is Recked" (1979) 13 U.B.C.L.R. 123, 156 described the Act as a complete misnomer.

143. McDonald "Electronic Surveillance in Crime Detection: An Analysis of Canadian Wiretapping Law" (1987) Dal H. L.J. 141, 141.

144. Supra at p.11 ff.

145. McDonald supra n144 at 141.

146. Ibid.

147. See Deutscher "The Protection of Privacy Act: Whose Privacy is it Protecting" in Gibson (ed.) "Aspects of Privacy Law" (1980), 142.

148. Supra at p.24.

149. Ibid.

150. Cohen "Invasion of Privacy: Police and Electronic Surveillance in Canada" (1982) 27 McGill L.J. 61q, 661 sets out a series of rules which police should satisfy before exercising their discretion to conduct surveillance.

151. Craig "Electronic Surveillance: Setting the Limits" (1975) 24 UNB L.J. 29, 29; Cohen supra n150 at 644, quotes the Quebec Police Commission: Inquiry on Organized Crime, Organized Crime and the World of Business" (1977), 2 the Commission found "organized crime is one of the greatest problems our society must face".

152. Duetscher supra n147 at 144.

153. Craig supra n151 at 39.

154. Borovoy "Centralized Data Identification and Intelligence" in Murray Information Processing and the Right to Privacy: A Crossroads Decision for North Americans (1972) 112.

155. (1980) 108 D.L.R. (3rd) 17. See generally McDonald supra n143 at 151.

156. Ibid 32.

157. McDonald supra n143 at 152.

158. Ibid citing R v Carothers; Richardson & Brunhoffer [1978] 6 W.W.R. 571.

159. R.S.C. 1985 cC-46, Section 144(2)(a)-(d)

160. Greenspan Commentator "Martin's Annual Criminal Code" (1989), 157 citing R v Playford (1984) 17 C.C.C. (3d) 454.

161. See "Present and Proposed Standards for Foreign Electronic Surveillance" (1976) 71 N.W.U.L.R. 109, 120 ff. U.S. statistics have shown that almost all warrants under the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S. (para. 2510-20) (1970) will be granted. In 1973 two applications out of 864 were refused; in 1972 four out of 855; in 1971 none out of 816.

162. See Dworkin "Hard Cases" (1975) 88 Harvard L.R.

1057 for a general discussion on theories of adjudication.

163. Lacovara "Presidential Power to Gather Intelligence: The Tension Between Article II and Amendment IV" (1976) 40 Law and Contemp. Problems 109, 127.

164. R.S.C. 1985 cC46, Section 195.

165. LaCovara supra n163 at 127. See also Nesson "Aspects of the Executive's Power over National Security Matters; Secrecy Classifications and Foreign Intelligence Wiretaps" (1973) 49 Indiana LJ 399, 415.

166. Lacovara Ibid 128.

167. R.S.C. 1985 cC46, Section 183.

168. Deutscher supra n147 at 162.

169. R.S.C. 1985, cC46, Section 185(1).

170. Ibid Section 185(c).

171. Ibid Section 185(e).

172. Ibid Section 185(d).

173. Ibid Section 185(e).

174. Ibid Section 185(f).

175. Ibid Section 186(1).

175a. Ibid Section 186(3)(e).

176. McDonald supra n143 at 159 citing McDonald

Commission Second Report, Vol. 2 at 1021.

177. R.S.C. 1985, cC46, Section 187.

178. Deutscher supra n147 at 162.

179. R.S.C. 1985, cC46, Section 187(1)(a)(ii).

180. See Greenspan supra n160 at 167; Deutscher supra n147 at 150 citing R v Miller and Thomas (1976) 32 C.R. (N.S.) 192, R v Welsh & Iannuzzi (No. 6) (1977) 32 C.C.C. (2d) 363, 371-72.

181. Greenspan Ibid 168.

182. (1988) 35 C.C.C. (3rd) 477; See also Re Zaduk and The Queen (1978) 98 D.L.R. (3rd) 133.

183. McDonald supra n143 at 160 citing U.K., Report of the Royal Commission on Criminal Procedure, 1981, 39.

184. S.C. 1976-77, c53, Section 178-13(2)(e).

185. (1986) 33 D.L.R. (4th) 744; See Greenspan supra n160 at 163.

186. (1983) 9 C.C.C. (3rd) 194. See Greenspan Ibid 162.

187. Ibid.

188. (1986) 33 D.L.R. (4th) 744. Greenspan Ibid 162.

189. (1985) 23 D.L.R. (4th) 532. See Greenspan Ibid 161.

190. R.S.C. 1985, cC34, Section 191.

191. See Deutscher supra n147 at 161.

192. R.S.C. 1985, c46, Section 196(2).

193. Ibid Section 196(3).

194. (1978) 98 D.L.R. (3rd) 133.

195. See Burns supra n142 at 142.

196. R.S.C. 1985 cC46, Sections 184, 193.

197. Ibid Section 194. See Burns "Electronic Eavesdropping and the Federal Response" (1975) 10 U.B.C. L.R. 36, 52 for a discussion of the constitutionality of the punitive damages provisions.

198. See definition of Crown in Crown Liability Act (1970) R.S.C., Section 2. "Her Majesty in Right of Canada". See Watt The Law of Electronic Surveillance in Canada (1979), 341.

199. Ibid.

200. See McDonald supra n143 at 148.

201. Ibid.

202. Only Watt supra n198 at 341 and McDonald supra n143 and 148 appear to discuss the matter at all.

203. McDonald Ibid.

204. Supra n198.

205. Ontario Law Reform Commission on Freedom of Information and Individual Privacy, Vol. 3, Protection of Privacy (1980), 159.

206. [1979] 4 W.W.R. 97. 115.

207. See Burns, supra n142 at 158.

208. R.S.C. 1985, cC46, Section 189(2).

209. See Burns, supra n142 at 149.

210. Burns Ibid 151.

211. Burns supra 197 at 60.

# CHAPTER V - PROVINCIAL LEGISLATION

## PART 1. INTRODUCTION

While we have criticized federal legislation and, in particular the Privacy Act, for failing to sufficiently regulate the informational process, such legislation could be regarded as a paradigm for provincial legislatives. With the exception of Ontario and Quebec, provincial legislatures have failed to provide any protection concerning the handling of information by government institutions.[1] The result has been that provincial government institutions are not required to conform to fair informational practices.[2]

Before we can confidently affirm our thesis in this area (i.e. the lack of provincial government initiatives has allowed the threats posed to civil liberties by advances in informational technology to go unchecked[3]), those provincial acts which purport to regulate some aspect of the informational process should be examined. These include: first, the Privacy acts of four provinces[4] which create a statutory tort of privacy; secondly, the Freedom of Information acts of six provinces[5] (which include, in the case of Ontario and Quebec, some regulation over the informational process); and thirdly, the Ombudsman acts, which can be used to challenge government actions and decisions.

## PART 2. THE PRIVACY ACTS OF BRITISH COLUMBIA, MANITOBA, SASKATCHEWAN AND NEWFOUNDLAND

The above-mentioned Acts create a statutory tort of invasion of privacy.[6] The Acts have not chosen a regulatory approach to privacy, rather the intention of the legislative has been to overcome the deficiencies in the common law.[7] It is suggested that the legislation will have little impact on government institutions and their use of informational technology. The reasoning is four-fold. First, there is the difficulty alluded to earlier in this paper, of an individual detecting an invasion of privacy caused by the handling of information by a government institution. Secondly, the Acts are unlikely, as we shall see, to support a broad interpretation of what constitutes an invasion of privacy. In particular, breaches of informational privacy standards are unlikely to be included. Thirdly, there are numerous broad defences to the tort of invasion of privacy. Fourthly, the cost of litigation is expensive (proceedings must be brought in the Supreme Court of the various provinces). An award of damages is likely to be relatively small, as there is no provision in any of the Act for exemplary damages.[8]

### (1) "Privacy" Under the Acts

Under the British Columbian Act, it is a tort, actionable without proof of damage, for a person wilfully and without claim of right to violate the privacy of another.[9] The Saskatchewan and Newfoundland Acts adopt a similar provision.[10] The Manitobian Act goes a little further and includes a negligent invasion of privacy,[11] although there is a defence if the defendant acted reasonably in violating privacy or did not, and should not have, reasonably known the act would have constituted an invasion of privacy.[12]

By not defining privacy, the Act, prima facie, allow considerable scope for judicial interpretation, and consequent adaption to changing social conditions.[13] However, the Acts prescribe a number of relevant factors.[14] Section 1(2) of the British Columbia Act states that:

> the nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, due regard being given to the lawful interest of others.[15]

The Manitoba, Saskatchewan and Newfoundland Acts also adopt a reasonableness test, although they do give specific examples of what may constitute an invasion of privacy.[16]

It is submitted that the reference to "lawful interests of others" in determining what is reasonable, restrict the applicability of this provision to cases involving the government handling of information. At the outset of this paper, we referred to the legitimate governmental interest in the efficient workings of various departments.[17] Such interests are lawful, and therefore likely to be considered as a reasonable invasion of privacy according to the Acts.

Judicial interpretation has also suggested a narrow interpretation of privacy under the Acts. In Davis v McCarthur,[18] the court had to consider whether certain acts of a private investigator, including attaching a bumper beeper to the plaintiff's motor vehicle, was an invasion of privacy. The court, both at first instance and on appeal, considered the surrounding circumstances (the purpose of the investigation, the right of the investigation, the conduct of the plaintiff, the extent of surveillance and its effect) in determining the nature and degree of privacy that was reasonable. At each instance, the court adopted a definition of privacy as the right to be left alone.[19] Employing this definition, the Court of Appeal concluded that:

> where he is not activated by malice or curiosity, and does not carry out his surveillance in an offensive way so as to attract public attention and does not make it so close and continuous as to go beyond reasonable bounds, he commits no breach of the Act.[20]

Lysk J in Silber v B.C.T.V. Broadcasting Systems Limited[21] also paid particular attention to the surrounding circumstances in considering what was reasonable. The fact that the alleged infringing act, namely the filming of events in a parking lot, was in a public place was crucial to his finding that there was no invasion of privacy.[22]

The restrictive approach evidenced in Davis and Silber, confirms that the Acts will have little impact in controlling modern informational practices, where information can be acquired and disseminated by less overtly intrusive methods. Government institutions are able to collect and use information without interfering with the "right to be left alone" definition of privacy. The effect of the Acts, is directed at the obtaining of information by undesirable means or preventing unwanted publicity, rather than informational privacy concerns.[23]

### (2) Exemptions Under the Acts

Furthermore, certain acts that otherwise constitute an invasion of privacy are specifically exempt. Three of these exemptions are particularly relevant to government institutions and the modern informational process.

First, there is no violation of privacy where there is consent of one of the parties.[24] In our earlier examination of the effect of the modern informational process, it was shown that the acquisition of vast amounts of information by government institutions was largely due to their increased ability to record transactions. However, the Acts provide little protection against the acquiring of information by such means, as the plaintiff normally consents to such acquisition of information.[25]

It might be possible to argue that consent for one purpose (i.e. to use the information in a particular way) does not create consent to use the information for another purpose.[26] This argument gains some support from the U.S. case of York v Storey,[27] in which a victim of assault, although consenting to photographs in the nude for the purpose of evidence in a criminal prosecution, was held to have had her privacy invaded, notwithstanding her consent, when the photographs were used for an extraneous prupose, namely the private gratification of other police officers.[28]

Clearly, the court in York was limiting the application of this principle to cases where the secondary use of the material was for an extraneous and private purpose. It remains to be seen whether Canadian courts will adopt such breach of confidence type principles and apply them irrespective of the nature of the secondary purpose.

It is submitted that, given the way in which the courts have interpreted privacy under the Acts, namely to protect unwanted publicity, that a second government institution which uses information in lawful manner will be able to rely upon the individual's consent in initially supplying the information. The basis of this submission is that this consent is likely to be characterized as permitting publicity to the extent of the handling of the information by government officials. There has been no further "publicity" when the information is passed to a second government institution and, therefore, the initial consent is unlikely to be vitiated.

Secondly, acts authorized by law do not constitute an invasion of privacy under the Act.[29] Prima facie this provision could authorize almost all actions of government institutions.[30] Government institutions are given certain statutory powers, therefore all acts in pursuance of such powers, even if invading privacy, would appear to be authorized by law.[31] There has been no judicial interpretation of this subsection. It is submitted that the phrase "authorized by law" permits no discretion on the part of the court and, therefore, renders irrelevant qualifications such as reasonableness or necessity.

A third exemption is the exclusion of acts or conduct (from constituting an invasion of privacy) of:

(i) A police officer acting in the course of his duty to prevent, discover or investigate crime or apprehend criminals;[32] or

(ii) A public officer engaged in the course of his duty under a law in force in the province;

providing such actions are not disproportionate to the crime or subject matter investigated, nor committed in the course of a trespass.[33]

Although this section does at least seek to qualify the exemption by imposing a test of proportionality, and the restriction that there be no trespass,[34] it is submitted that these qualifications assume little relevance to modern informational technology, which does not require trespass or even direct surveillance to gather information about an individual. In the absence of direct surveillance, it is unlikely that use of information by a law enforcement authority can be said to be disproportionate to the crime or investigation.[35]

### (3) Conclusion

Experience has shown that the provincial Privacy acts have been very sparingly used, and not at all with government institutions as a defendant. This has led Burns to suggest that the passing of these Acts is a non-development.[36] While it might be argued that this is not conclusive of the ineffectiveness of these Acts, and that the deterrence aspect is important (i.e., people regulating their own behaviour because of the Acts), any such "deterrence" is unlikely to extend to government institutions. First, privacy, as used in the Act, is likely to give rise to a narrow interpretation, inapplicable to the modern informational process. Secondly, the broad exemptions in the Act create, as Ryan says:

> an almost blanket exemption in favour of what may be termed duly constituted authority ... the Privacy Act amounts to a virtual licence for government invasion of privacy, cast in the form of protection.[37]

The provincial Privacy Acts, therefore, fail to provide individuals with any protection against unfair handling of information by government institutions.

## PART 3. PROVINCIAL FREEDOM OF INFORMATION ACTS

A number of provinces, namely Ontario, Nova Scotia, Newfoundland, New Brunswick, Manitoba and Quebec, have enacted freedom of information legislation.[38] Because these acts raise identical issues to those that we discussed in relation to the federal Privacy Act and Access to Information Act, we do not propose to consider these provincial acts in detail, but rather intend only to highlight their main features.

The procedure for obtaining access under the provincial acts is similar to that of the federal Acts. In the first instance, the individual makes an application to the particular government institution for access to information. The head of the institution determines wehther or not to grant the request. If he refuses, then an independent mediator (the Ombudsman in the case of Manitoba, New Brunswick and Newfoundland;[39] the Information Commissioner in the case of Ontario and Quebec;[40] a House of Assembly Committee in the case of Nova Scotia[41]) investigate the matter and the reasons for non-disclosure, and make recommendations as to whether or not access ought to be given.[42] Under all Acts, except Ontario, New Brunswick and Nova Scotia, an appeal lies to a court if non-disclosure is maintained.[43]

However, all of the Acts suffer from the same defects as the federal Privacy Act and Access to Information Acts. In particular, there are broad exceptions to access where the information relates to cabinet records, law enforcement, defence and international affairs and inter-governmental affairs.[44] Further, in none of the acts do we find any concept of an expanded right of access, which requires the individual to be notified on the occurrence of certain events.[45] The provincial acts can therefore be subjected to the same criticism as we made in respect of the federal acts, namely the reliance upon the individual to initiate matters by making a request to the particular institution.

Only the Ontario and Quebec Acts include provisions requiring government institutions to observe certain standards in relation to their handling of personal information.[46] These provisions are

---

substantially similar to sections 4-8 of the federal Privacy Act. However, our two main criticisms of that Act are equally applicable to the provincial Acts. There is a complete lack of enforceability of the enacted standards and a failure to include an express right of privacy.[47]

In one respect, the Ontario and Quebec Acts do answer one of our criticisms of the federal Privacy Act, and that is they require only information that is necessary for the proper administration of a lawfully authorized activity be collected[48] (except in the case of the Ontario Act of law enforcement collection of information[49]). As we discussed previously, the federal Privacy Act does not contain such a relevance test.[50]

Both the Ontario and Quebec Acts also regulate the disclosure of information.[51] In each case the categories of disclosure are similar to those contained in the federal Privacy Act, although there is no equivalent provision to section 8(2)(m) of the federal Privacy Act, which permits disclosure when the head of the institution is of the opinion that the interest in disclosure clearly outweighs the interest of the individual in privacy.

Lastly, the Manitoba, Ontario and Quebec Acts contain provisions for the indexing of personal information databanks.[52]

## PART 4. THE OMBUDSMAN ACT

The office of Ombudsman has been introduced into all provinces, with the exception of Prince Edward Island.[53] The Ombudsman's mandate is to investigate the administrative acts of provincial government departments[54] and to enable him to do so, he is armed with powers of access to government information,[55] summonsing and examination of government employees or other persons on oath,[56] and entry onto premises.[57]

The Ombudsman, through the use of these powers, prima facie, can overcome some of the problems associated with the modern informational process, in particular the secrecy of government departments[58] and the powerlessness of individual citizens against the organs of State.[59]

However, the office of Ombudsman has been in existence for some considerable period of time,[60] long before the specific problems caused by the modern informational process. One might therefore expect that the Ombudsman, both in practice and due to its statutory restrictions, is not well equipped to control government databanks.[61]

### (1) Jurisdiction of Ombudsman

The first limit of the Ombudsman's effectiveness in this area arises from his jurisdiction. Using section 11 of the Albertan Act as a model,[62] the Ombudsman only has jurisdiction:

> to investigate any decision or recommendation made ... or any act done or omitted, relating to a matter of administration and affecting any person or body of persons in his or its personal capacity, in or by a department or agency, or by an officer, employee or member thereof in the eercise of any power or function conferred on him by any enactment.[62]

The courts have widely interpreted "matters of administration" and it is likely it would include matters associated with databanks. In British Columbia Development Corporation et' al v Ombudsman and Attorney-General of British Columbia,[63] the Supreme Court of Canada held that matters of administration included:

> all conduct engaged in or by government authority in furtherance of government activities.[64]

The informational process appears to fall within such a description.

However, the effect of section 11 on informational practices is greatly reduced by the requirement that the act or decision must affect a person(s) in his personal capacity.[65] Such a requirement clearly suggests that the Ombudsman's jurisdiction is limited to investigating individual complaints,[66] rather than a general investigation of government practices. The scheme of the Act supports his interpretation. Section 14 refers to the Ombudsman not investigating complaints if the complainant does not have a sufficient personal interest: section 17(5) and section 21 refer to various consents and notices that must be given to the complainant. All of these provisions assume that the individual has an interest in the complaint, which would be lacking under a general review. The recurring problem arises that the individual will be left unaware of any government abuses of information and will therefore be unlikely to initiate a complaint.

## (2) Exclusions of Jurisdiction

In addition to this inherent restriction on jurisdiction, there are a number of exclusions of the Ombudsman's jurisdiction relevant to the informational process.[67] First, under section 12 of the Act, the Ombudsman's jurisdiction is ousted when the decision or act is reviewable on the merits by way of appeal, or objection or review by a court or tribunal. Therefore, a refusal of access to information will, in most cases, be excluded from consideration by the Ombudsman because under the federal Privacy and Access to Information Acts, as well as the provincial Freedom of Information Acts, a procedure exists for review. Whether a review by the Ombudsman is permitted where the individual's complaint relates to the handling of information by a government institution is more doubtful. Clearly, there is no review under any of the Privacy or Access Acts, but one might be able to say that the individual, in some instances, has a remedy under the common law (eg. for defamation, breach of confidence, etc.). The question is, does the possibility of bringing such an action affect the Ombudsman's jurisdiction.

One could argue that the intention of section 12 is to exclude all cases where the Ombudsman's decision may conflict with the judiciary and therefore, where there is any possibility of a common law action, no appeal lies to the Ombudsman. The opposing argument seems stronger. Judicial review is distinguishable from a review of the merits in that it is not considering the administrative correctness or fairness of the decision, and possibly substituting its decision for that of the government institution, but is concerned with the legality of the decision. The court in Re Ombudsman of Ontario and Health Disciplines Board[68] advanced such reasons in holding that a judicial review was not a review on the merits.

The Ombudsman's influence is also limited in that he must make certain findings before he can make any recommendations in respect of a complaint.[69] The first such finding that he may make is that the act or decision is contrary to law.[70] Such a requirement assumes little relevance to the modern informational process, where the information can easily be acquired legally, and where, as we have seen, there are no laws governing the use to which it may be put.

Secondly, a finding may be made that the decision or act was "unreasonable, unjust, oppressive or improperly discriminatory".[71] Government informational policy is generally to prevent such occurrences, the same being inconsistent with "efficient administration". Invasion of privacy per se does not appear to fit into any of the above categories.

The third finding that the Ombudsman may make is that the decision of the government institution was based wholly or partly on a mistake of fact or law.[72] Obviously, therefore, use of true information by a government institution is excluded from the operation of this subsection. However, use of true information is one of the major concerns of modern informational technology. There is the further difficulty of discovering the use of an inaccurate fact by a government institution.

The Ombudsman's remedial powers are lastly validated if he is of the opinion that the decision of the government institution was "wrong".[72a] Prima facie, "wrong" suggests some unjustness or error in the decision or act, and as such would not allow a mere substitution of the Ombudsman of his own decision on a particular complaint for that of the government institution. However, section 20 appears to cover error in section 20(1)(c) (mistake of law or fact) and unjustness in section 20(2) (irrelevant grounds or improper purpose). Therefore, one could argue that "wrong" must be given a wide interpretation, if it is to have relevance in the context of section 20, and that this meaning must be to allow the Ombudsman to substitute his view for that of the government institution.

### (3) Enforcement Procedures

Perhaps the most significant restriction on the Ombudsman's functions is his lack of enforcement powers. He only has the power to make recommendations to a particular government department.[73] The department is under no obligation to follow any such recommendation and the Ombudsman has no legal means to compel it to do so.[74] In such circumstances, the Ombudsman can only include such matters in a report to Parliament,[75] or alternatively in his annual report.[76] In particular instances, the threat of these political remedies may be sufficient for a government institution to reverse a particular decision, but because of the individual nature of the complaints, it is unlikely to effect the general administrative practices of the departments and how they deal with information.

### (4) Conclusion

The Ombudsman is a good example of an Act intended for a particular purpose, namely enabling individuals to have an increased capacity to challenge decisions of government departments, but which has some incidental effect on certain aspects of informational practices. Statistics confirm this role - most complaints to the Ombudsman concern either an explanation for a decision or a reversal of that decision and only 2.3% deal with a desire to verify information held on file.[77]

However, any protection afforded by the Ombudsman is sporadic and not productive of any coherent theory. Lack of jurisdiction and weak enforcement powers are partly responsible. Equally important are the practical limitations on the Ombudsman - his resources are simply inadequate to control government databanks.[78] This was recognized by the Kingston Conference on Computers as long ago as 1970, when it was held that the number of databanks would necessitate the creation of several Ombudsmen.[79] If this was done, it would be inappropriate to laden these officials with the restrictions imposed by the present Ombudsman Act.

# FOOTNOTES - CHAPTER V

1. Rankin "Privacy and Technology: A Canadian Perspective" (1984) 22 Alta. L.R. 323, 336.

2. Ontario Commission on Freedom of Information and Individual Privacy, Vol. 3, Protection of Privacy (1980) 138.

3. Flaherty "Protecting Privacy in Police Information Systems: Data Protection in the Canadian Police Information Centre" (1986) 36 U of T. L.J. 116, 121 suggests that the absence of data protection at the provincial level has meant that police information systems are developing without adequate external oversight, legislative or otherwise, to protect privacy.

4. The Privacy Act, R.S.B.C. 1979, c336; The Privacy Act, R.S.M. 1987, c.P125; The Privacy Act R.S.S. 1978, c.P24; The Privacy Act, S. Nfld. 1981, c6.

5. See generally Mann Computer Technology and the Law in Canada (1987), 219 ff. See S.O. 1987, c25; S.N.S. 1977, c10; S. Nfld. 1981, c5; S.N.B. 1978, cR-10-3; S.M. 1985, c6; S.Q. 1982, c30.

6. Fridman Introduction to the Law of Torts (1978) 166.

7. Ibid.

8. Burns "The Law and Privacy: A Canadian Experience" (1976) 54 Can B.R. 1, 38.

9. Ibid. See The Privacy Act, R.S.B.C. 1979, c336, s1(1).

10. See Geddes "Private Investigator and the Right to Privacy" (1989) 27 Alta. L.R. 256, 294; The Privacy Act R.S.S. 1978, cP24, s2; The Privacy Act, S. Nfld. 1981, c6, s3(1).

11. Geddes Ibid S.M. 1985, c6, s5(6).

12. Ibid.

13. Burns supra n8 at 11.

14. Osborne "The Privacy Acts of British Columbia, Manitoba and Saskatchewan" in Gibson "Aspects of Privacy Law" (1980), 87 suggests that the Acts go too far in listing factors to be taken into account.

15. The Privacy Act R.S.S. 1978, cP24, s6(1) is almost in indentical terms.

16. R.S.S. 1978, cP24, s3; R.S.M. 1987, cP125, s3; S. Nfld. 1981, c5, s4.

17. Supra at p.1.

18. (1970) 17 D.L.R. (3rd) 760.

19. Ibid 765. At first instance see (1969) 72 W.W.R. 69, 73.

20. (1978) 17 D.L.R. (3rd) 760, 763.

21. [1986] 2 W.W.R. 609.

22. Ibid 615.

23. McLaughlin "Educational Records and the Right to Privacy" (1981) 15 U.B.C.L.R. 175, 176.

24. The Privacy Act B.C., supra n4, s3(1); The Privacy Act, Manitoba, supra n4, s5(1); The Privacy Act, Saskatchewan, supra n4, s4(1)(a); The Privacy Act, Nfld., supra n4, s5(1).

25. Osborne supra n14 at 90.

26. Ibid.

27. (1963) 324 F. 2d 450; See Osborne Ibid.

28. Ibid.

29. The Privacy Act B.C., supra n4, s2(1)(c); The Privacy Act, Saskatchewan, supra n4, s4(1)(c); The Privacy Act, Manitoba, supra n4, s5(d); The Privacy Act, Nfld., supra n4, s5(1)(c).

30. Osborne supra n14 at 95 cites Ryan in Ontario Law Reform Commission, Report on Protection of Privacy in Ontario (1968), 69 as saying this section gives a virtual carte blanche to duly elected authorities to invade privacy.

31. Osborne Ibid.

32. The Privacy Act B.C., supra n4, s2(1)(d); The Privacy Act, Saskatchewan, supra n4, s4(1)(d); The Privacy Act, Manitoba, supra n4, s5(e); The Privacy Act, Nfld., supra n4, s5(1)(d).

33. Ibid.

34. Osborne supra n14 at 95.

36. Burns supra n8 at 32.

37. Osborne supra n14 citing Ryan supra n30.

38. Supra n5.

39. S. Nfld. supra n5, s12; S.N.B. supra n5, s7; S. Manitoba supra n5, s14.

40. S.O. supra n5, s50; S.Q. supra n5, s135.

41. S.N.S. supra n5, s13.

42. See generally Mann supra n5 at 219 ff.

43. S. Nfld. supra n5, s14: S.M. supra n5, s27; S.Q. supra n5, s147.

44. eg. see S.O. supra n5, ss12-22.

45. See supra at p.105.

46. S.O. supra n5, ss37-43; S.Q. supra n5, ss64-79.

47. Supra at p.116.

48. S.O. supra n5, s38(2); S.Q. supra n5, s64.

49. S.O. supra n5, s38(2).

50. Supra at p.107.

51. S.O. supra n5, s42; S.Q. supra n5, s59.

52. S.O. supra n5, ss44-46; S.Q. supra n5, s132; S.M. supra n5, s50.

53. See Ontario Commission on Freedom of Information and Individual Privacy supra n2 at 143; For the various Ombudsman Acts see R.S.N.B. 1973, c0-5; R.S.Q. 1977, cP-32; C.C.S.M. c0-45; S.N.S. 1970-71, c3; R.S.S. 1978, c0-4; R.S.O. 1980, c325; R.S.N. 1970, c285; R.S.B.C. 1979, c304; R.S.A. 1980, c0-7.

54. There is no federal Ombudsman. "Crown" in the various Ombudsman Acts has been held to mean Crown in the right of the Provinces, not Canada; See Re Ombudsman Act [1974] 5 W.W.R. 176.

55. Using the Albertan Act as a model. Ombudsman Act, R.S.A. 1980, c0-7, s17(1).

56. Ibid s17(3).

57. Ibid s25.

58. See Ontario Commission on Freedom of Information and Individual Privacy, supra n2 at 93.

59. Maloney "The Ombudsman Idea" (1979) 13 U.B.C.L.R. 380, 382 refers to the commonly held view of the Ombudsman as the watchdog of the bureaucracy.

60. Ibid 381. The first Canadian province to establish an Ombudsman was Alberta in 1967. The Swedish Ombudsman dated back to 1809.

61. Jacob "Some Legislative Proposals for the Proper Regulation of Databanks" in Rowe (ed) Privacy Computers and You (1972), 143 argues the Ombudsman cannot be the complete answer to the privacy problem.

62. R.S.A. 1980, c0-7, s11.

63. [1985] 1 W.W.R. 193.

64. Ibid 213. The Ontario Court of Appeal in Re Ombudsman of Ontario and the Health Disciplinary Board of Ontario (1980) 26 O.R. (2nd) 105, 123 also gives a wide definition of matters of administration "I think that the most reasonable approach to administration is to regard it as a compendious description of the wide range of government activities carried on by bodies other than legislature and the courts."

65. Ontario Commission on Freedom of Information and Individual Privacy, supra n2 at 124.

66. Although the Ombudsman himself may initiate a complaint himself. See R.S.A. 1980 c0-7, s11(2).

67. See generally Sawer "The Ombudsman Comes to

Alberta" (1968) 6 Alta. L.R. 95, 97.

68. (1979) 95 D.L.R. (3rd) 716, 723.

69. See Sawer supra n67 at 97.

70. R.S.A. 1980, c0-7, s20(1)(a).

71. Ibid s20(1)(b).

72. Ibid s20(1)(c).

72a. Ibid s20(1)(d).

73. Ibid s20(3).

74. Maloney supra n59 at 386.

75. Ibid R.S.A. 1980, c0-7, s20(4).

76. Ibid s27.

77. Ontario Commission on Freedom of Information and Individual Privacy, supra n2 at 127.

78. Jacob supra n61 at 143.

79. Ibid.

# CHAPTER VI - PROTECTION FROM ADVANCES IN INFORMATIONAL TECHNOLOGY UNDER THE CANADIAN CHARTER OF RIGHTS AND FREEDOMS

## PART 1. INTRODUCTION

The inability of the common and statutory law to adequately protect the individual from the impact of advances in informational technology clearly suggests that the Canadian Charter of Rights and Freedoms will play a critical role in filling this hiatus. As Mackay says, the enactment of the Charter has given the courts a bold new mandate to measure the acts of the legislative and executive against the standards of the Charter.[1] The protection afforded by the Charter will not only apply to federal and provincial legislation,[2] but will apply to all acts of government bodies exercising statutory authority, including any action which depends for its validity on statutory authority (eg. through regulations, by-laws, etc.).[3]

The Charter is broadly worded[4] and contains no express reference to informational technology or even privacy.[5] The courts will therefore be left with the task of adapting and expanding the traditional, broad provisions of the Charter to solve the new problems of modern society, such as informational technology.[6] To date there have been few Charter cases dealing directly with issues relating to the use of information. We must therefore look to the general theory behind the relevant Charter provisions and analyze Unites States' cases for assistance.

Direct protection from informational technology will only be found if there is a right of privacy in the Charter. It will further depend on any such right of privacy being sufficiently broad to include informational privacy.

Unlike some of the International Conventions protecting human rights,[7] the Charter contains no express right of privacy.[8] There are, however, indications from the courts that section 7 of the Charter, the right to "life, liberty and security of the person", might be interpreted as implying a right of privacy.[9] What must be examined is the protection afforded by section 7 specifically against advances in informational technology.

The Charter will also provide incidental protection against certain aspects of the informational process. This will occur when interests protected under the Charter are infringed by some aspect of the informational process. Such provisions therefore will not offer any general theory of protection to the individual in the area of informational technology.

The most relevant sections of the Charter in this category are section 8, the right to be free from unreasonable search and seizure, and section 2(b), freedom of expression. The impact of section 8 is obviously restricted to regulating certain forms of acquisition of information. Section 2(b) has a more indirect influence; the acquisition or maintenance of information may inhibit (or chill) an individual's freedom of expression, and thus infringe section 2(b). Such a chill could also arise under section 2(d), freedom of association, where an individual might be inhibited from associating with other persons through fear of information being acquired concerning that association and used later to his detriment.[10] Further, section 2(b) is relevant in determining an individual's right of access to information, both of a personal and public nature, held by the government.[11]

Informational privacy contains three fundamental rights:[12]

(i) Personal Privacy: The right of the individual to decide what information to show to others;

(ii) Personal Access: The right of the individual to know how, when and why data is being collected about him;

(iii) Public Access: The right of people to access public information to monitor the activities of government.

Sections 7, 8 and 2(b) have been chosen for detailed examination because they place an important role in securing the aforementioned rights. Section 7 is relevant both to personal privacy and personal access in that it might give the individual some control over personal information. Section 8 will have an impact on personal privacy by restricting the acquisition of information by government institutions. Section 2(b) is relevant to securing public and personal access to information, and also personal privacy, by preventing the individual from being inhibited from sharing information with others.

## PART 2.- SECTION 7

### (1) Introduction

section 7 Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice

Section 7 of the Charter will play a critical role in protecting individuals from the consequences of advances in informational technology. Informational technology, as demonstrated in Chapter II,[13] has provided government institutions with a valuable new tool, information, causing a consequent loss of power to the individual and encroachment into new areas of individual lives.[14] On the other hand, section 7 is concerned with the dignity and worth of the individual.[15] As held in R.L. Crain Inc. v Couture,[16] it gives constitutional recognition to the principle that the individual is sovereign and there are

---

limits to the exercise of governmental authority over the individual. As Calvin says, it invokes "cherished ideals of civil liberties".[17] The potential conflict betwen the informational process and section 7 is thus readily apparent.

The extent of protection will depend on judicial interpretation of the phrase "life, liberty and security of the person" and, in particular, whether it encompasses a right of privacy. It will also depend on how the limitations inherent in section 7 (i.e. not to be deprived of the enunciated rights except in accordance with the principles of fundamental justice) and also in section 1 of the Charter are interpreted in informational cases.

### (2) Judicial Interpretation of Section 7 to Date

The Supreme Court of Canada in Morgentaler v The Queen[18] stated that the boundaries of section 7 have not been firmly established and that it would be unwise at this stage of charter adjudication to attempt to do so. However, certain principles have clearly emerged. These principles, insofar as they relate to the informational process, can be summarized as follows:

(i) Section 7, like all Charter provisions, should be interpreted broadly, not legalistically.[18a] The task of the court is:

> to secure for persons the full benefit of the Charter's protection whilst avoiding

adjudication on the merits of public policy

Lamer J in Reference re Section 94(2) of the Motor Vehicles Act approving Dickson J (as he then was) in R v Big M Drug Mart Ltd.)[19]

(ii) Each of the rights in section 7 (of "life", "liberty", and "security of the person") are distinct though related concepts.[20] Therefore, although an independent meaning can be ascribed to each right, they each have a mutual and reciprocative influence on each other.[21] The right not to be deprived of the rights set out in section 7 except in accordance with the principles of fundamental justice, is not a separate right but is a qualifier of the other rights in section 7.[22] The rights set out in sections 8-14 of the Charter are specific examples of infringements of section 7.[23]

(iii) The definition of "liberty" in section 7 extends beyond a mere freedom from bodily restraint. Until about 1985, there was considerable academic and judicial debate about this issue,[24] but since that time a broader definition of liberty has been adopted. The first stage of this process occurred in R v Robson,[25] where Nemitz J of the British Columbian Court of Appeal adopted broad United States' court definitions of liberty[26] and held that:

> liberty under law extends to the full range of conduct which the individual is free to pursue and it cannot be restrained except for property government objective.

The Supreme Court of Canada in Re Singh and Minister of Employment and Immigration[27] approved the wider definition of liberty, by adopting Stewart J in Board of Regents of State College v Roth that:

> liberty not only meant freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of life, to acquire useful knowledge, to marry, establish a home, bring up children according to the dictates of his own conscience and generally to enjoy those privileges long recognized as essential to the ordinary pursuit of happiness by free men.[28]

The above decisions defind liberty in terms of a right to be left alone, especially when making important personal decisions. Wilson J in Morgentaler v The Queen[30] took a similar approach when she held that liberty guaranteed to every individual a degree of personal autonomy over important personal decisions.[31] Her reasoning in reaching this conclusion was two-fold; first, the idea that the Charter in its entirety and not just section 7, was based on the concept of maintaining the dignity of the individual;[32] secondly, a review of U.S. authorities, particularly the abortion cases which had given a degree of personal autonomy to the individual.[33] Although Wilson J gave a minority judgment in Morgentaler, her definition of liberty has been subsequently expressly adopted by the British Columbian Court of Appeal in Wilson v Medical Services Commission of B.C.[34] and at least impliedly by the

Nova Scotian Supreme Court in Re Maritime Medical Care Inc. and Khaliq-Kareeml.[35] It is clear, however, from the majority judgment of Dickson CJC in Morgentaler[36] that he considered the boundaries of liberty not to be finally determined and that it was neither necessary or wise in Morgentaler to speculate as to the limits of these boundaries.

(iv) The interpretation of "security of the person" in section 7 has also moved away from earlier pronouncements, limiting it to protection of the bodily integrity of the individual in the physical context.[37] One of the earliest pronouncements to this effect was in R v Robson,[38] where it was held that security of the person included a right to an area of privacy to which the State must not make arbitrary or unjustifiable intrusions. The Supreme Court of Canada followed this approach in Re Singh and Minister of Employment and Immigration.[39] Although the ratio of that case was that a minimum security of the person encompassed freedom from physcial punishment, or the threat thereof,[40] it is apparent that wider definitions were contemplated. Wilson J approved the wider definition proposed by the Law Reform Commission that security of the person included not only physical integrity, but also provisions necessary for its support.[41] Any doubt as to a restrictive interpretation of security of the person was dispelled by the Supreme Court of Canada in Morgentaler,[42] where separate judgments of both

Dickson CJC and Wilson J, applied to section 7, earlier definitions of security of the person in section 11 made by Lamer J in Mills v The Queen.[43] Lamer J held that security of the person protected both state interference with bodily integrity and serious state imposed psychological stress, at least in the criminal law context. This psychological stress could occur (in relation to the pending criminal accusations) through stigmatization of the accused, loss of privacy, stress and anxiety resulting from a multitude of factors including possible disruption of family, social life and work, legal costs and uncertainty as to the outcome and sanction.[44] Again the majority reasons of Dickson CJC in Morgentaler stressed that it was not necessary to consider whether security of the person extended further to include interests unrelated to personal autonomy, such as a right to privacy or interests unrelated to criminal justice.[45]

(v) The Supreme Court of Canada in Reference re Section 94(2) of the Motor Vehicles Act[46] established that the review required by the second limb of section 7 (not to be deprived of rights except in accordance with the principles of fundamental justice) was performed by an analysis of the content of the impugned legislation to see if it accorded with the principles of fundamental justice. This review included a procedural aspect,[47] (equivalent to natural justice) but in addition, the substance of the legislation had to be considered[48] to see if it "corresponded with the basic tenets of our legal systems", which may be presumptions in common law or expressed in international conventions of human rights.[49] The court in R.L. Crain Inc. v Couture listed four considerations for this review: the historical developments of rights protected by the common law, the legislation tradition in Canada as found in existing legislation; community standards or the living tradition; and the need for compelling factors to justify placing the collective interest of society ahead of the rights of the individual.[50]

(vi) As yet, there has been no authoritative decision recognizing a right of privacy within the ambit of section 7. In Morgentaler,[51] Dickson CJC declined to express an opinion whether a right to privacy was encompassed in either "liberty" or "security of the person", saying it was too early in Charter adjudication to express an all encompassing definition of section 7. The proponderence of authority in the lower courts support the exclusion of the right of privacy from section 7. (See R v Rowbotham,[52] Charboneau et al v College of Physicians and Surgeons of Ontario,[53] and K. Mart Canada Ltd. v Millmont Developments Ltd.).[54] On the other hand, the court in R.L. Crain v Couiture[55] referred to an area of privacy being included in the concept of security of the person (rather similar to the zones of privacy theory of Douglas J in Griswold v Conneticut.)[56] The minority decision of Wilson J in Morgentaler with its reference to section 7 protecting personal autonomy comes close. It is submitted, to adopting a family based definition of privacy.

(vii) Once an infringement of section 7 is found, it is still open for the court to find that the impugned act or legislation was justified under section 1 of the Charter as a reasonable limit in a free and democratic society. (Reference Re Section 92(2) of the Motor Vehicles Act)[57]

### (3) Protection Afforded Against Informational Technology by the Current Definition of Section 7

The foregoing analysis of section 7 reveals several areas in the informational process where government practices may infringe section 7.

Acts of physical surveillance undertaken by government, or alternatively the legislative scheme authorizing such surveillance, could be found invalid unless complying with the principles of fundamental justice. It would seem undeniable that acts of physical surveillance overcome the threshold test of section 7 in that the individual's liberty is infringed in that his personal autonomy has been interfered with.[58] Alternatively, his security of the person has been impaired in that there has been disruption of his personal environment.

The surveillance must then be reviewed against the principles of fundamental justice. Although the validity of each act of surveillance or the legislation authorizing it will depend on its particular circumstances, one can foresee that breaches of the principles of fundamental justice might occur. For example, in R v Carriere,[59] it was held that writs of assistance[60] offended the principles of fundamental justice by virtue of the absence of judicial scrutiny and the broad unreviewable grounds upon which they could be issued. Further, in R v Findlay and Grellette,[61] the validity of Part IV of the Criminal Code, (then embodying the Protection of Privacy Act)[62] was considered, although ultimately upheld as the court took the view that the safeguards set out in Part IV of the Code were sufficient. As we shall examine later,[62] section 186 of the Code (which provides for confidentiality of records) has been examined for fairness according to section 8 of the Charter, with the result that the accused has been allowed access to the sealed package if required for his defence.[63]

What is important for present purposes is the willingness of the courts to examine legislation for compliance with the principles of fundamental justice.

Examination of cases where a search has been held to be unreasonable under section 8 of the Charter will give further guidance as to when surveillance might infringe the principles of fundamental justice. Given the correlation between section 7 and section 8 and, in particular, that a breach of section 8 has been held to be a specific example of a breach of section 7 (security of the person), an unreasonable search and seizure must be one which infringes the principles of fundamental justice. What consitutes an unreasonable search and seizure will be considered later.[65]

The present definitions of both liberty and security of the person do not, it is submitted, apply to other techniques used by government institutions to gather data, such as linkage of databanks or the recording of individual's actions and transactions.[66] In many instances when data is collected in this way, the government has relied on the voluntary supply of information by the individual. There has been no infringement of the individual's personal autonomy as required by the definition of liberty, as the act being complained of, namely the supply of information, was exercised through the choice of the individual. Likewise, security of the person has not been infringed; it being unnecessary to invade the individual's bodily integrity to gain the information. The present interpretation of section 7 is therefore simply too narrow to catch such behaviour.

Even if no consent can be found, indirect acquisition of information by government (such as a linkage of databanks and recording of transactions), is unlikely to infringe section 7. The threshold test of there being a breach of liberty or security of the person will not be satisfied. The widest definition of liberty to date has been Wilson J's in Morgentaler which allows a degree of autonomy in the individual over important personal decisions such as abortion. Clearly, under the current interpretation the personal choice does not extend to control of information. Likewise, when the information has already been imparted by the individual, it would appear too late to subsequently argue that there had been an infringement of security of the person.

In certain circumstances, the maintenance of information (as distinct from its acquisition) might infringe section 7. If an individual is labelled by data (eg. as a criminal) and it is clear that this information is likely to be used, then arguably security of the person may be infringed. The Morgentaler definition of securty of the person[67] clearly encompasses a label which stigmatizes an individual, although the application of the definition would have to be extended to the non-criminal area.

United States cases where the maintenance of information has infringed the fourteenth Amendment, generally relate to expungement of arrest records.[68] For example, in Manard v Saxbe,[69] expungement of the defendant's records was ordered (the defendant was arrested but never charged with an offence), the court holding that the record constituted undoubted social stigma that would cause him detriment (eg. in employment). Therefore, the fourteenth amendment was infringed. Provided the Morgentaler decision is extended to the non-criminal arena, it is submitted that a similar result would be reached in Canada. However, if an applicant could not show likelihood that the information, even if stigmatizing him, was likely to be used, there would be difficulties in establishing that the applicant had standing under the Charter to bring an action. The problems caused by standing will be discussed later.[70]

Section 7 will also have some impact on dissemination of information, particularly when it labels the individual in some way. Again the individual's bodily integrity is impaired by the ensuing stigma. Canadian cases have yet to consider this aspect of section 7; however, in the United States there have been several cases dealing with the dissemination of information and the fourteenth amendment.[71]

In Wisconsin v Constantineau[72] the court held that before dissemination occurred affecting a person's good name, reputation, honour or integrity (the information in question described a serious illness of the applicant), procedural due process demanded that the applicant be given an opportunity to be heard. The principles of fundamental justice demand not only procedural review but also substantive review, therefore suggesting that

Canadian courts would reach a similar decision.

A problem would arise if the information being disseminated related solely to the individual's reputation. Re Kodellas and Saskatchewan Human Rights Commission[73] suggests an individual's reputation is not included as part of security of the person. The fine distinction between reputation and stigma is illustrated in the United States case of Paul v Davis.[74] In that case, the United States Supreme Court held that circulating to shopowners lists of known shoplifters, including on it the name of the defendant who had been arrested but never convicted; although possibly defamatory, did not infringe the fourteenth amendment because liberty did not include reputation "as a candidate for protection over and above other interests protected by State law".

It is suggested that Canadian Courts could well come to a different conclusion. What the applicant suffered in Paul v Davis was not merely damage to reputation, but also stigmatization (i.e. his character was tarnished by false statements). The U.S. Supreme Court in Paul v Davis however, by categorizing the injury as one to reputation, excluded it from protection. Justice Rehnquist's reasoning was two-fold; first, other interests are more compelling than reputation; secondly, there are zones of privacy, inferring that reputation was on the outer of such zones and therefore more likely to be displaced.[75] In Canada, the presence of section 1 of the Charter is likely to avoid such a rigid distinction between stigma, deserving of protection, and reputation being excluded from protection. The arguments of Justice Rehnquist are better directed in determining whether the impugned act or legislation is a reasonable limit under section 1, rather than at the stage of examination for a breach of security of the person. Justice Rehnquist, of course, was not able to do this, there being no equivalent of section 1 in the U.S. Bill of Rights.

There are, however, two pervading and serious limitations as to the degree of protection offered against informational technology provided by the current definition of section 7.

The first of these limitations, inherent in however widely section 7 is defined, are procedural difficulties.

Under the Charter, an application has three remedies from which to select;[76] exclusion of evidence under section 24(2);[77] a declaration that particular legislation is invalid under section 52(i);[78] and most relevant in the informational context, section 24(1), which provides:

> Anyone whose rights or freedoms as guaranteed by this Charter have been infringed or denied

> may apply to a court of competent jurisdiction to obtain such remedy as the Court considers appropriate and just in the circumstances.

Section 24(1) poses several difficulties for the applicant. First, he must become aware of the infringement of his rights or freedoms. In the case of information being acquired and maintained by the government, this presents a real difficulty for the applicant, as he may not even know of the fact of the acquisition of the information. The Charter is not designed to assist a litigant in becoming aware of an infringement of his rights. Even if he overcomes this hurdle, the litigant must be able to provide that his rights have been infringed, before section 24(1) can be invoked.[79]

Apart from obvious evidentiary problems, a crucial issue in the context of informational technology is whether mere maintenance of information can in any circumstances lead to a breach of section 7. If it can, the individual will have the right to bring such applications under section 24(1); if not, any action brought will be struck out for lack of standing.

Canadian cases have not yet had to consider this issue. The United States' courts have held that unless the application can show that it is likely that the information will be used to the detriment of the individual, as with the expungement of records cases discussed previously,[80] standing will be denied. In Finlay v Hampton[81] it was held that while an applicant may be unhappy about the presence of adverse and untrue information in a file, the courts would not strike such material from the file or take any action in the absence of a real threat of injury. At the time of action, the court held that any future action was merely speculative. The earlier U.S. case of Green v McLean[82] reached a similar conclusion; an adverse security report per se did not infringe the individual's rights. The issue of due process only became relevant if and when the security clearance was revoked.

One would hope that the Canadian Courts might come to a different conclusion. A person's liberty might be said to be infringed by the holding of information, in that it dissuades him from engaging in the full range of legitimate activities, because of fear that the information might be used against him. Security of the person could also be said to be infringed at the time an individual is labelled by untrue or inaccurate information. The wording of section 24(1) does not require, it is submitted, actual objective harm befall an applicant before an action can be instituted, rather only an infringement of rights or freedom. The purpose of the Charter, as has been repeatedly emphasized, is to secure the protection of the Charter provisions for all individuals.[83] Technical denial of standing does not accord with such a philosophy.

The second major limitation, restricting the applicability of section 7 to the informational process, is the narrowness of the present definition. As has been demonstrated, informational processes are only regulated when they pose a threat to the individual's autonomy or physical or psychological well being in the personal sense (eg. in preventing the individual exercising his personal decisions). Section 7 does not, according to its present definition, extend beyond this autonomy in the personal sense to give the individual control over personal information and, through this control, regulate the informational process directly. It is submitted that what is required is that a right of privacy be enunciated as being within the parameters of section 7. A right of privacy which includes this informational component becomes a foil to the growth of information.[84] It makes deprivation of the individual's control over information loss of a constitutionally protected right. A right of privacy is thus in direct conflict with the informational process and can be used as a challenge to prevailing informational practices. The circumstances of the deprivation of the individual's control over information must be scrutinized for constitutional fairness.

Apart from its impact on the informational process, which we shall consider below, a right of privacy in the Charter would also help create the belief in the individual in the fair handling of information by government institutions, which we have argued is so essential to the protection of civil liberties.[85] It does so because it gives the individual the constitutionally protected right to challenge government actions or even legislation in relation to the handling of information, thus giving the individual the means to satisfy himself that personal information is being handled fairly. A right of privacy would also impose a corresponding duty[86] on the government official, thus potentially influencing his behaviour in handling information.

A right of privacy will obviously have far greater impact on the informational process than the current interpretation of section 7. For example, in respect to maintenance of information, arguments of standing would be rendered obsolete[87] as the individual has lost control over information, a protected right, which would be sufficient to invoke section 24(1). Acquisition of information, even if supplied voluntarily, may also violate a right of privacy in that the information is unnecessary is used for a different purpose than the one for which it was supplied. In such a case, there has been interference with the individual's control over the information. Dissemination, even of true information, might infringe a right of privacy as it represents total disregard for any interest the individual might possess in the confidentiality of the information.

Two U.S. cases illustrate how, in practice, a right of privacy might lead to a more rigorous examination of informational practices.[88] In Californian Bankers Association v Schulz,[89] one of the judges of the court, although declaring valid the Bank Secrecy Act which required that microfilm copies of cheques be made, held that if the legislation had applied to all cheques and not just cheques over $10,000.00, then the legislation would have been invalid as an infringement of privacy because financial transactions reveal much about a person's activities, associations and beliefs. Schulz illustrates how the dissemination of true information may require a balancing of the need for that information against the privacy of the individual.

In Whalen v Rose,[90] legislation which required the names of persons using a certain drug on a doctor's prescription to be recorded and held in a centralized government computer file, was held to be valid on the grounds that it was a valid objective and not an unwarranted denial of privacy. However, the court went on to say that it was:

> not unaware of the threat to privacy implied in the accumulation of vast amounts of personal information in computer data banks.

The court further held that if there had been disclosure of the information, as distinct from just collection, it might have reached a different conclusion. Again in Rose, the acquisition of information is being measured against the need for it. In neither Schulz nor Rose would section 7, without a right of privacy, have posed any threat to the impugned legislation.

### (4) A Right of Privacy Under Section 7 of the Charter and Its Consequences for Informational Technology

Given then demonstrated advantages to declaring section 7 to include a right of privacy, the next task is to examine the likelihood of such a judicial declaration, and how such a right would operate in the Charter framework. As stated previously, the Supreme Court of Canada in Morgentaler v The Queen[91] declined to set out the parameters of the definitions of either liberty or security of the person, and in particular declined to say if a right of privacy was included. In contrast, the U.S. Supreme Court has long recognized an implied right of privacy in the U.S. Bill of Rights. The first expression of this came in Griswold v Conneticut[92] where a right of privacy was found in matrimonial affairs. Various sources of this right were expressed; Douglas J finding zones of privacy in the first, third, fourth, fifth, and ninth amendments; Goldberg and Brennan JJ finding the right in the ninth amendments; Harlan J in the fourteenth amendment. Later cases expanded the right of privacy to the non-matrimonial arena.[93] In Roe v Wade,[94] the U.S. Supreme Court confirmed that the source of a right of privacy was the fourteenth amendment.[95] It should be noted that recent cases of the U.S. Supreme Court, in particular William L. Webster and The Attorney-General of Missouri[96] and Bowers v Hardwick,[97] although not overruling Roe v Wade,[98] have restricted its application.[98] (eg. in Hardwick it was held that the right of privacy did not shield homosexual acts from criminal law[99] and in Webster, statutory imposed restrictions on abortion were permitted.)

The decisions of the lower courts in Canada have rejected section 7 as including an implied right of privacy. Two reasons have been advanced. First, a separate right of privacy was considered but expressly rejected by the Joint Committee on the Repatriation of the Constitution and should not, therefore, be implied (R v Rowbotham).[100] Therefore, while an earlier draft of the Charter had contained a right of privacy, the final draft did not. Secondly, it has been held that any right of privacy exists under section 8 of the Charter and not section 7 (Charboneau v College of Physicians).[101]

Both of these reasons can be easily refuted. As Elliott says,[102] one should use great caution in using earlier drafts of the Charter as a guide to interpretation because of ambiguity behind changes in wording. He cites as an example the right of privacy. Was it removed because the draftsman thought it unnecessary to provide an express right, or was it removed, as claimed in Rowbotham, because it was rejected. Further, in determining that the review contemplated in section 7 was not limited to procedural due process, the court was not influenced by the fact that the Joint Committee had suggested only procedural due process.[103] Therefore, the rejection of the Committee finding in one area should mean that they can be equally rejected in another.

Secondly, the proposition that a right of privacy could be found in section 8 and not section 7 of the Charter was said to be based on the decision of the Supreme Court of Canada in Hunter v Southam.[104] One could argue that Southam did not say this at all, it merely recognizing a right of privacy (in a particular form) existed in section 8, but not to the exclusion of section 7. Even if Southam does suggest this, it is clearly inconsistent with the later decision of the Supreme Court in Morgentaler, where the court was clearly of the opinion that a right of privacy could exist in section 7. Further, Reference re Section 94(2) of the Motor Vehicles Act clearly holds that section 8 is a specific example of a breach of section 7. As such, a right of privacy found in section 8 could not operate to exclude that right from section 7.[103]

One is therefore left with the unarticulated reason of public policy for the rejection of an implied right of privacy. No reasons are proferred in support of this denial. It is suggested that the dangers of informational technology, set out in Chapter II, require a right of privacy. Problems of unworkable application in practice of a right of privacy in section 7 can be overcome, it is suggested, through the use of a qualifier in section 7 and the application of section 1 of the Charter. U.S. experience has not suggested that a right of privacy is unworkable in practice.

It is submitted that the better interpretation of the Charter and decided cases also supports the incorporation of a right of privacy. The reasoning is six-fold:

(i) The courts have firmly pronounced that Charter rights and freedom must be interpreted broadly and not narrowly and legalistically (R v Big M Drug Mart Ltd.).[106] Extension of a right to tackle problems of modern society shculd be encouraged in light of such an approach. Denial of a right of privacy by reference to external aids such as earlier drafts, is excessively legalistic.

(ii) Respect for the inherent dignity of the individual and his role and place in society are the precepts on which the Charter is based (Dickson CJC in R v Oakes).[107] Privacy is also fundamental to such concepts, it being designed to ensure individual sovereignty and autonomy in the face of government intervention. This was even recognized in R v Rowbotham,[108] where it was held that a right of privacy is the underlying concept behind the Charter and finds its expression in many of the Charter rights and freedoms. It seems illogical to protect certain values enshrined in the Charter, but to deny protection to the value of privacy, acknowledged as the basis for the inclusion of the other rights.

(iii) To date, the underlying reasoning behind the interpretation of section 7 has been to give the individual a measure of protection in his or her private life from government intrusion. This is close to what might be called a "family based right of privacy".[109] It requires only a small extension to make the definition applicable to issues such as informational technology.

(iv) A right to privacy has found protection in various International instruments. The European Convention for the Protection of Human Rights and Fundamental Freedom,[110] the Universal Declaration of Human Rights,[111] and the International Convenant on Civil and Political Rights,[112] all contain an express right of privacy. Wilson J (diss) in Jones v The Queen[113] clearly recognizes the relevance of international instruments and quoted extensively from them. The fact of acceptance of a right of privacy in influential international instruments clearly will be a persuasive influence upon the decision of the Supreme Court of Canada when it is called upon to determine if a right of privacy exists in the Charter.

(v) Section 7 of the Charter is more receptive to an expansive interpretation of liberty and security of the person, which includes a right of privacy, than the 14th Amendment of the U.S. Bill of Rights, where a right of privacy has been implied.[114] The U.S. Courts do not have an equivalent to section 1 of the Charter and, therefore, the interpretation adopted in the 14th Amendment must make due allowance for legitimate government aims and conflicting rights. Such allowance can be made under Charter adjudicated in the section 1 examination rather than in section 7.

(vi) In R v Dyment,[115] the Supreme Court of Canada recognized a right of privacy in section 8. As a breach of section 8 is a specific breach of section 7, logically to the extent of that overlap, section 7 must also contain a right of privacy. Dyment specifically included privacy, in the informational sense, as being protected under section 8.[116] Indeed, there would seem to be no reason why this right of informational privacy should not be extended to section 7 to all aspects of the informational process.

It is beyond the scope of this paper to consider the appropriate formulation of this right of privacy (especially insofar as it relates to the personal and territorial apsect of privacy). However, it is clear from our preceding discussion that we consider the right of privacy as being the key for the individual developing autonomy, free from governmental influences.[117] In the informational sense, this means that a right of privacy under section 7 should give the individual a certain element of control over personal information. In Westin's words, the individual should have the right "to determine for themselves, when, how and to what extent information about them is committed to others".[118]

Section 7, of course, is not infringed if the individual is deprived of his rights (in this case the right of privacy) in accordance with the principles of fundamental justice. The issue in the informational context is to determine what meaning to ascribe to this phrase. Cases to date have only dealt with the application of the principles of fundamental justice in the context of the criminal law. Presumably, the government will argue that if information is supplied voluntarily, or if it is true, then it cannot infringe the principles of fundamental justice. Fundamental justice, the argument would follow, demands some unfairness on the part of the government, not present in consensual acquisition of information or acquisition of true information. R.L. Crain v Couture[119] provides a measure of support to that argument. The court held that the principles of fundamental justice are found by reviewing the protection of the impugned rights at common law, in existing analogous legislation and the general community attitudes to the right in question. The common and statutory law have placed little control over true or voluntarily supplied information.

It is submitted, however, that the courts are better able to meaningfully apply the principles of fundamental justice to the informational process. The courts have held that the principles of fundamental justice are not static and will evolve in response to changing perceptions of what is arbitrary, unfair or unjust.[120] We discussed previously the adoption of principles of data protection as being the standards by which the informational process is judged.[121] It is submitted that the principles of data protection can be used in Charter adjudication to determine if a denial of privacy has been made in accordance with the principles of fundamental justice. The data protection principles, in whatever form they are adopted by the courts, become the standards in determining whether the right to privacy has been taken away in an arbitrary or unfair or unjust manner.

Section 1 of the Charter provides a further avenue for the government to justify an infringement of the right of privacy. The universally accepted rules[122] governing the application of section 1 were laid down by Dickson J (as he then was) in R v Oakes.[123]

The government bears the burden of proof to show that the proposed limit on an individual's rights is reasonable and to do so must establish:

(i) That its objective is sufficiently important to warrant overruling a constitutionally protected right. This a high standard, which must relate to pressing and substantial concerns;

(ii) The means chosen must be reasonable and demonstrably justified. Dickson J (as he then was) explained this as a form of proportionality test, requiring the balancing of the interests of society and the individual. There are three components to the proportionality test; first, the means adopted must be designed to achieve the objective in question and must not be arbitrary, unfair or based on irrational considerations - in short they must be "rationally connected to the objective"; the means must impair as little as possible on the rights or freedom in question; thirdly, there must be proportionality between the effects of the means and the objective.

Of course, the application of this test to informational cases will largely depend on the particular facts of each case. However, certain general results may be predicted. First, mere administrative expediency, that is the pursuit by a government department of objectives, will not normally be sufficient to deprive an individual of his rights. In the words of Lamer J in Reference re Section 94(2) of the Motor Vehicles Act "only in exceptional cases will the rights under section 7 be sacrificed to administrative expediency".[124] Administrative expediency fails to safisfy the first part of Dickson's J test in R v Oakes of establishing a sufficiently important government objective. This will often be the case where information is routinely collected.

However, section 1 may be more readily used in circumstances where the government is able to point to a legitimate goal which it is seeking to achieve. In the informational context, the individual's right to privacy will often conflict with legitimate government objectives of law enforcement and the health, safety and welfare of citizens, or even other protected rights in the Charter. Where the government has such legitimate aims, the first element of the Oakes test is satisfied; however, the proportionality test may still be infringed. In cases involving law enforcement, it will be easier to satisfy the proportionality test because the objective is of such importance. Stringent government measures are therefore more likely to be considered necessary, and appropriate (i.e. proportional) in the circumstances.

The conflict between the general government objective of the health, welfare and safety of its citizens and the individual's right of privacy is more acute. For example, in the United States, it has been held that a statute requiring a mother on welfare to provide the name of the father of illegitimate children and answer various other intimate questions was valid in that the objective of the enquiry was to enforce a monetary obligation and not interfere with the individual's privacy.[125] This has lead various writers to suggest that the welfare recipient has no expectation of privacy.[126]

There is some authority in Canada that suggests that a conflict between a valid government objective (such as welfare) and a protected right, is relevant in establishing whether the right has been infringed. Thus, in Zutphen Brothers Construction Ltd. v Dywidag Systems,[127] the court held that the concept of liberty had to take into account the political realities of the modern state. Likewise, in Re MacTavish[128] the Alberta Queen's Bench held that in some cases section 7 requires an obvious balancing of competing rights.

It is submitted, contrary to the above cases, that the proper approach is not to say that welfare recipients or any able group per se do not have a right of privacy, or that there had been no denial of that right because of competing rights. Rather, such consideration should be directed at section 1, where it can be examined whether the government objective is being achieved in the best way possible. R.L. Crain v Couture[129] support this approach, where it held that because of restrictions provided by section 1, it was unnecessary to read any further restrictions into the definition of section 7. Wilson J in Morgentaler also followed this approach. She examined the state's objective in protecting the fetus in the context of section 1 and said that there would come a point where the state's interest prevailed.

Logically, there approach of Crain and Wilson J in Morgentaler appears correct. A breach of section 7 has occurred, irrespective of whether there is some justification for it. If, therefore, section 1 is used in this way, in relation to the health and welfare conflict with section 7, it will lead, in many instances, to informational practices being improved so as to comply with the proportionality test and infringe upon the privacy of the individual as little as possible. If, however, the enquiry is directed only at considering whether a breach of section 7 has occurred, the government does not have the onus of satisfying the proportionality test.

## (5) Conclusion

The foregoing analysis reveals that the impact of section 7 on informational technology, will depend on whether a right to privacy can be implied into the phrase "life, liberty and security of the person". If it can, section 7 will play a useful role in the informational context. A right of privacy in section 7 would, of course, not be a complete panacea to the problems caused by informational technology. The major procedural and evidentiary problems would remain. On the other hand, if section 7 is not interpreted widely, it will include at its widest a form of "right to be left alone" style of privacy, which has only marginal relevance to the informational process. The informational process will only be peripherally regulated, where its interests coincide with some protected rights.

## PART 3. SECTION 8

### (1) Introduction

Section 8 Everyone has the right to be secure against unreasonable search or seizure

Somewhat surprisingly, section 8, which deals with only one aspect of the informational process, namely the gathering of information,[130] is further advanced in developing principles permitting the individual to have some control over the acquisition of personal information by government institutions, than section 7, which has the potential to regulate all aspects of the informational process. This is perhaps because the judicial interpretation of section 8 has focused on the conflict between legitimate governmental objectives on the one hand, and the right of the individual to be free from government intrusion on the other.

In his seminal judgment in Hunter v Southam Inc.,[131] Dickson J (as he then was) held that the primary purpose of section 8 was not restricted to the protection of property, but included the broader right of the protection of individuals from unjustified intrusions upon their privacy. This, he said whether:

> expressed negatively as freedom from unreasonable search or seizure or positively as an entitlement to a reasonable expectation of privacy indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by the government must give way to the governmental interest in intruding on the individual's privacy in order to advance its goals notably those of law enforcement.[132]

The effect that this assessment will have upon the informational process will depend on two issues.[133] The first is what forms af acquisition of information are subject to section 8: that is, what constitutes a search or seizure. It will be important to establish that the more intrusive forms of acquisition of information, such as electronic surveillance, fall within section 8. Also important will be determining the status of demands for information or the voluntary supply of information in the administrative context. The second issue that arises is determining the appropriate standard of reasonableness under section 8. Again, the application of this standard to administrative area will be of crucial importance.

Section 8 requires reasonableness of search and seizure in two ways.[134] First, the legislative scheme authorizing a particular search or seizure must be reasonable. Secondly, the particular search or seizure, although authorized by a valid statute, must be carried out in a reasonable manner.

### (2) What Constitutes a Search or Seizure

The Supreme Court of Canada in Hunter v Southam, by adopting the decision of Stewart J in Katz v U.S.,[135] that section 8 protected "people not places", clearly indicated a broad approach to the question of what constitutes a search or seizure. In Southam, the court focussed on the intrusion by the government in an area where the individual had a reasonable expectation of privacy, rather than comparing the nature of that intrusion with the concepts of search and seizure.[136] Reid and Young suggest that, in light of this approach, one can predict that:

> while some generic link between an activity that intrudes on privacy and search or seizure (is required) ... there can be no question that an activity cannot escape the bounds of section 8 simply because it is labelled as something other than search or seizure.[137]

### (a) Electronic Surveillance

The application of section 8 to electronic surveillance is important to informational technology, given the intrusiveness of such surveillance. The court in R v Rowbotham[138] held that electronic interception of private communications came within section 8. The Attorney-Generals for Canada and Ontario conceded this point in R v Finlay & Grellette,[139] a concession with which the court agreed.[140] The same concession was made in R v Thompson.[141] After these decisions and Southam, there is no prospect of successfully arguing the contrary. Clearly, wiretapping is more invasion of personal privacy than a conventional search.[142] As was stated by Goodman J.A. in R v Playford,[143] wiretapping may occur over a lengthy period of time without the knowledge of the subject of surveillance, and further it gathers intimate personal details not only about the subject, but also concerning third parties. Wiretapping also has the necessary link with search or seizure in that it involves the search and seizure of something tangible, namely communications. The United States reached the same conclusion in Katz.[144]

Similarly, the Ontario Court of Appeal in R v Wong,[145] held that video surveillance was a search and seizure, provided that in the circumstances there was expectation of privacy. The court found that there was no logical distinction between electronic interception of conversations and video surveillance. Rather, the occurrence of a search or seizure depended on the individual's expectation of privacy.[146]

However, in the United States, there has been some movement in the area of electronic surveillance, to require a stronger nexus between the intrusion and the wording of the Fourth Amendment ("persons, houses, papers and effects").[147] This has been evident in electronic monitoring cases and also cases involving interception of communications between an agent and informer. In both instances, no search or seizure was found.

In _U.S._ v _Knotts_,[148] the United States Supreme Court held that monitoring signals from a radio transmitter was not a search and seizure. The radio transmitter was inserted into a container, which it was known that the applicant was intending to purchase. After completing the purchase, the applicant placed the container in his motor vehicle. The transmitter then tracked the route of the motor vehicle to its ultimate destination, a cabin-dwelling. There was no interception of communications. The court reasoned that a person travelling in a motor vehicle had a lower or no expectation of privacy and likewise, could have no such expectation relating to movements of objects, such as a container, within that vehicle.[149] Further, as visual surveillance would have been permitted, then the use of electronic surveillance to perform the same function was not unreasonable.[150]

It is suggested that Canadian courts would not follow Knotts. What the court in Knotts failed to recognize was the differing aspects of privacy. Therefore, whilst an individual might not have had an expectation of privacy in the personal sense regarding his presence in the car (he being in "plain view"), he does have an expectation of privacy in the informational sense, relating to personal information which might be acquired from the vehicle. The tracking of the vehicle to its destination, it is submitted, falls into this latter category.

The Supreme Court of Canada in R v Dyment[151] recognized that privacy had an informational, as well as personal, aspect. Further, Southam requires a non-technical approach to search and seizure. Therefore, given the intrusion by the police in inserting the tracking device and the type of personal information being derived from this intrusion, it would appear likely that a sufficient expectation of privacy exists, requiring the police to obtain a warrant. Indeed, one can see no reason why it was not possible for the police to obtain a warrant. The further argument of the court in Knotts that visual surveillance would have been permitted is surely irrelevant. Just as overhearing a conversation does not require a warrant but wiretapping does, there is good reason to distinguish, as the Ontario Court of Appeal did in R v Wong, between visual and video surveillance.

In the case of police informers or undercover agents secretly recording a conversation with an accused, the United States' courts have held that the fourth amendment does not apply.[152] The reasoning of the Supreme Court in U.S. v White[153] was that the subject of the interception had no legitimate interest of privacy, merely because he held the misplaced view that the person to whom he confided personal information would not reveal that information to the police.[154] It therefore made no difference whether that revelation to the police occurred at some later stage (as in the case when a conversation is normally repeated), or occurred instantaneously, as with the case of electronic interception and relaying of communications.[155]

Again, the decision in Dyment might suggest that these cases might not be followed in Canada. As we shall later examine,[156] Dyment suggests that if information has been given in confidence to one party, then the relaying of that information to a third party can constitute a search and seizure, provided that the individual had a reasonable expectation of privacy in relation to the information. In other words, the consent is limited to the initial purpose for which the information was supplied.

As a result, therefore, of the decision of the

Supreme Court of Canada in Southam and Dyment, one can expect that in most cases electronic surveillance will be a search and seizure for the purposes of section 8. This obviously will have an impact on law enforcement authorities, which are the government bodies most likely to resort to the acquisition of information using such devices. Their use of eelctronic devices to acquire information, can now be scrutinized for reasonableness.

### (b) Administrative Searches and Seizures

The applicability of section 8 to the administrative area, where the government acquires vast amounts of information on individuals, is also of importance.

The discovery of the "generic link"[157] between the acquisition of information by government and search and seizure, may be more difficult to find in the administrative area. Two questions arise:

(i) When are administrative demands for information a search and seizure within section 8;[158]

(ii) Can there be a search or seizure notwithstanding that the information was voluntarily supplied.

Government bodies heavily rely on the acquisition of information in these ways[159] and the applicability of section 8 will directly affect informational practices.

### (i) Administrative Demands for Information

There are two conflicting lines of authority concerning the issue whether a demand for information can be a search or seizure. Cases which have held there to be a search or seizure[160] have relied on the decision by the Albertan Court of Appeal in Alberta Human Rights Commissioner v Alberta Blue Cross Plan.[161] That case involved a request for records belonging to an employer in connection with a preliminary investigation of a sexual discrimination complaint. The court simply held (without any detailed reasoning):

> that a forced production of documents in a civil proceeding or during an administrative enquiry, is a search or seizure.

In the circumstances however, the seizure was reasonable.[162] McDonald J in Re Reich and College of Physicians & Surgeons of Alberta (No. 2),[163] felt bound by this decision, but distinguished it on the basis that it only applied to cases where production was ordered by the court and not to a demand for information under the Medical Profession Act where there was no element of forced production.

The stronger line of authority however, suggests that a demand for information is not a search or seizure. The leading case in Re Ziegler and Hunter,[164] where the Federal Court of Appeal rejected the Alberta Blue Cross decision as being without reason or authority. The Federal

Court of Appeal held that the essential charactistics of a search or seizure consisted of forcible entry, without warning, into someone's home or business. No such characteristics were present in the case of a subpoena duces tecum.

Ziegler was applied in R v Oldfield[165] where a demand for information under the Tax Act, was held to have none of the characteristics of search and seizure such as unwanted entry and the taking of goods.[166] The Ontario Court of Appeal in Thomson Newspapers Limited v Director of Investigation and Research[167] followed the Ziegler line of authorities, although it introduced the qualification that a demand was not a search or seizure if there was a reasonable opportunity for the applicant to challenge the order before it took effect. Subsequent cases have also accepted this qualification of Ziegler.[168]

As Stone points out,[169] the Alberta Court in Gainers Inc. v United Food and Commercial Workers International Union[170] distinguished its earlier decision in the Alberta Blue Cross case. It did so on the basis that in the Alberta Blue Cross case the documents were sought by the Albertan Human Rights Commission, which administered, investigated and decided whether or not to prosecute in respect of alleged offences. The court found that the facts in Gainers were quite different, as they involved documents that were sought pursuant to statutory powers of testimonial compulsion by an administrate agency.[171] Even if there was a seizure, the court held that it was reasonable, in that it required rational deliberation by the Labour Board before the order was issued and, further, because the purpose of the order was to assist in determining the veracity of witnesses.[172]

It is submitted that the Ziegler line of cases is too restrictive and not in accordance with the approach set out in Southam. One should focus not on whether a demand is technically a seizure, but on the reasonable expectation of the privacy of the individual. As Finklestein says,[173] if its purpose is to protect privacy, section 8 should apply where a demand for information accomplishes the same purpose as a search or seizure (i.e. the production of records). Therefore, demands for information of a public nature would not be a search or seizure, but demands for private information may be.[174] In cases involving production of documents pursuant to a court order, it is suggested that where the order is directed at a party to the proceedings, there is no search and seizure, there being no reasonable expectation of privacy. On the other hand, where the order is directed at a third party, such a reasonable expectation of privacy is more likely to exist. Nevertheless, an order in such circumstances is likely to be reasonable, perhaps as an exception to a warrant requirement, if appropriate grounds exist to challenge the order.

This approach would concentrate on the privacy aspects of section 8 and not solely on the degree of physical intrusion.[175] It would open up whole areas of acquisition of information by government, to scrutinization for reasonableness. The Supreme Court of Canada in Dyment[176] perhaps hinted that it would reach the same conclusion in relation to demands for information, when it focussed on the confidentiality of the information in question in that case, rather than emphasizing the means by which it was obtained.

### (ii) Voluntary Supply of Information

Another area important in the context of acquisition of information is the voluntary supply of information by the individual. It has been stated that in such cases, there is no search and seizure as the victim has consented to the acquisition of the information.[177] The issue is whether an individual might have a reasonable expectation of privacy when he has abandoned his "exclusiveness" in relation to that information.

However, the consent argument fails to recognize that information, although provided voluntarily, was done so only for a particular purpose. If that information can be used for other purposes, without the consent of the supplier, then the supplier has lost control over that information.

There is some indication that the Supreme Court of

Canada has recognized this problem. In R v Dyment,[178] a physician took from the defendant a blood sample without his consent. The physician later handed the sample to a police officer, again without the consent of the defendant. The court found the acquisition by the police of the sample to be an unreasonable seizure. Lamer J (Beetz and Wilson JJ concurring) held that when the physician gave the blood to the police, he was subject to a duty to respect the defendant's privacy. Therefore, the receipt of the blood by the police was a seizure. This judgment indicates that even if the individual had consented to the original sample being taken by the physician, this consent was limited to the physician.

The judgment of La Forest J (Dickson CJC concurring)[179] in Dyment reached the same conclusion, although its reasoning was wider. La Forest J held that the privacy protected by section 8 included informational privacy. This was the right of the individual to communicate or refrain from communicating information about himself or herself. Given this right, the individual could expect that information:

> should remain confidential to the persons to whom and restricted to, the purposes for which it is divulged[180]

La Forest J therefore, held that even if consent had been given by the defendant to the physician to take the sample of blood, this consent was limited to the use of the sample for medical purposes and did not permit divulgence to the police.

The decision in *Dyment* is to be welcomed. It focuses on the individual's expectation of privacy in relation to the particular information. It will have important implications for the informational process in restricting the use of information (even though supplid voluntarily) to the purpose for which it was supplied. Therefore, one could expect an individual to be able to challenge a government department, which has obtained personal information about that individual through the linkage of databanks. *Dyment* fully accords with one of the essential principles of data control, namely that the use of information is restricted to the purpose for which it was supplied.

### (3) Reasonableness of the Search or Seizure

A search or seizure will only infringe section 8 if it is unreasonable. The standard of reasonableness that is adopted will also have a significant impact on the informational process by making government bodies comply with this standard before acquiring information.

The general test is one of reasonableness.[181] Dickson J (as he then was) in *Southam* laid down three specific rules, non-compliance with which indicated that the search was prima *facie* invalid:[182]

(i) Wherever possible, the search or seizure must be approved by way of prior judicial authorization, although this might not be reasonable in all cases;

(ii) The person granting the authorization need not be a judge, but they must act in a judicial manner;

(iii) There must be reasonable and probable grounds that an offence has been committed and that evidence of this is likely ~~to be~~ found.

Clearly this warrant requirement creates barriers to the acquisition of information by government. At the very least, it ensures further accountability of government officials, who must justify their need for information. Southam however, was a quasi-criminal case and it is of some importance how its criteria will apply in the administrative area.

### (a) Reasonableness of Administrative Search and Seizure

There have been two related justifications, given by courts in refusing to follow Southam into the administrative area.[183] These justifications are said to act as a rebuttal of the presumption that warrantless searches are unreasonable.[184] First, the courts have adoped the qualifier stated in Southam, that the warrant system must be feasible. Thus, it has been held that warrants in the administrative area are not feasible.[185] The second stated justification is that there is a lower expectation of privacy on the part of individuals subjected to an administrative search and seizure and therefore it is reasonable to permit government intrusion without a warrant. This has been held as the justification for warrantless searches at international borders.[186]

The distinction between law enforcement and administrative searches and seizures was first raised in R v Rao[187] (pre Southam). In that case, Martin J.A. held that there was a clear distinction between a search and seizure in the law enforcement context and that of an administrative search and seizure for audit purposes for regulation of business activities. Re Belgoma Transportation Limited and Director of Employment Standards[188] and Re Quesnel[189] made the same distinction, holding that spot audits were aimed not at detecting criminal activity, but ensuring compliance with a regulatory act.

Cases subsequent to Southam have followed this distinction. In Bertram S. Miller v The Queen,[189a] the court held that a warrantless search under the Plant Quarantine Act was reasonable. In reaching this conclusion, the court held that the reasonableness of an administrative search depended on the following criteria: the purpose of the statute by which the search and seizure was authorized, the nature of the thing searched or seized, the place where the search took place, and the expectation of the public at large and of the individual subject to the search and seizure.[190] Applying these considerations, the court held that a routine administrative search carried out for public health and welfare objectives (in that case preservation of forests) was reasonable without a warrant requirement.[191]

The scope of warrantless administrative searches was extended even further in R v Bichel,[192] where it was held that administrative searches without warrant, were reasonable even if it involved a search of the residence of the individual.[193] The court held that a warrantless administrative search was reasonable because the search must occur at a reasonable time, the subject of the search could ask the inspector to return at a more convenient time, there was minimum intrusion into privacy, no stigma attached to the search and the inspection must proceed on a routine basis. A warrant therefore would be futile as it would not provide the individual with any greater protection and would bring the administration of justice into disrepute by being a mere rubber-stamping exercise.[194]

Administrative searches without warrant will not be permitted when they involve a quasi-criminal investigation. In such cases, the Southam criteria apply.[195]

The Supreme Court of Canada has not yet had cause to consider the distinction between law enforcement and administrative searches and seizure. However, in R v Simmons,[196] the court gave a warning that it might consider administrative searches and seizures more strictly than the lower courts. Dickson CJC, in considering the reasonableness of a customs search at Toronto Internatinal Airport, held that it would be incorrect to place "an overwhelming emphasis on the surrounding circumstances when assessing the reasonableness under section 8" and that only in exceedingly rare situations should the warrant requirements of Southam be departed from.[197] A border search (if properly carried out)[198] constituted one of those rare exceptions, due partly to the individual's lower expectation of privacy, but also because of the strong interest of the state in preventing illegal goods coming into the country.

It is submitted that the arguments for the administrative exception to the warrant requirement are unconvincing. While a warrant may well be a rubber-stamping, as suggested in R v Bichel,[199] it still serves a useful function in that it provides a permanent record which can provide a basis for subsequent examination of the reasonableness of the intrusion. Further, the mind of the government official is turned to the need for the intrusion, before it takes place, thus creating an internal check that the criteria for intrusion are justified. The lesser expectation of privacy argument ignores the nature of the information that may be acquired. An individual does have a reasonable expectation of privacy in relation to personal information or confidential business information, even if it is to be used in an administrative context.

Of course, there will be occasions when a warrant is not feasible. Re Milton and The Queen,[200], involving the seizing of fishing nets, is one such case. However, this does not justify a complete exception to the warrant requirement of administrative search and seizures. As Reid and Young argue,[201] what is required is some flexibility and an awareness that where the search is more random or more personal, a warrant requirement is necessary. The modification of the law relating to the sufficiency of law enforcement warrants,[202] suggest how administrative warrants may prove useful:

(i) The purpose of the search and seizure should be described in the warrant with partcularlity including a statement setting out the type of information sought in the search;

(ii) The legal justification for the search should be detailed including the giving of notice of the right of the subject of the warrant to challenge the validity of the search or seizure before it occurs;

(iii) The grounds upon which the informant believed the search to be necessary and no more intrusive than necessary should be specified. Included in this requirement would be details of prior routine inspections, the location and time of the search etc.

If the above criteria are adopted to administrative searches and seizures, the importance of the information gained is recognized. The government is potentially made accountable for any abuses which may have occurred in acquiring the information.

### (b) Reasonable and Probable Grounds for the Commission of an Offence

The third of Dickson CJC criteria in Hunter v Southam[203] also has an impact on the informational process of government institutions. Not only must the particular government institution seeking the warrant in each instance satisfy a judge or other independent arbitrator that these are reasonable grounds to believe that an offence has been committed, but also the statutory scheme by which a warrant is issued also must comply with this standard.

Therefore, for example, the provisions of Part VI of the Criminal Code[284] which authorizes electronic surveillance can be scrutinized according to this standard. This was the issue in R v Finlay and Grellette,[285] where the court held that the statutory scheme authorizing the issuance of the warrant was valid, even though it did not expressly state that a warrant must only issue on establishing that there were reasonable grounds to believe that an offence had been committed. The court held that the test used in the Code, namely that authorization for a warrant would be granted "if in the best interests of the administration of justice" was a sufficient test as it was fundamental that the best interests of justice would not be served if a warrant was issued on a lower standard, such as the suspicion of an offence.

### (4) Applicability of Section 1 of the Charter

The relationship between section 1 and section 8 is yet to be clarified. In Southam,[286a] Dickson J (as he then was) said he did not have to consider the relationship between section 8 and section 1 and would leave to another day:

> the difficult question of the relationship between those two sections and more particularly what further balancing of interests, if any, may be contemplated by

section 1, beyond that envisaged by section 8.

In both R v Noble[207] and Re Reich and College of Physicians & Surgeons of Alberta (No. 3),[208] the court held that section 1 supplied no further test. In most cases concerning section 8, no argument is presented by the Crown concerning section 1.[209]

The only case where a section 1 has been applied is R v Rachow,[210] where the Albertan Court of Appeal held that even assuming that a search of the driver of a motor vehicle, as part of a campaign to detect impaired drivers, was a search under section 8, it could be justified under section 1. The court in Rachow did not clarify its reasoning and there would appear to be no reason why the search could not have been justified under the reasonableness test in section 8.

The inclusion of the proportionality test in section 1, appears to make it a stricter test than the reasonableness test in section 8. Proportionality requires that less intrusive forms of intrusion be considered, notwithstanding that the search may otherwise be reasonable. In R v Finlay and Grellette,[211] the court held that a general requirement of minimization in relation to section 8 was too onerous and should not be imposed on criminal law enforcement officials, though in a particular instance a judge could order minimization procedures. It would therefore appear unlikely that anything that was unreasonable under section 8 could be saved under section 1.

## (5) Section 8 and a Right of Privacy

It is clear that Dickson J (as he then was) in Southam, viewed section 8 as inextricably linked to a right of privacy. Dickson J expressed this as the individual's reasonable expectation of privacy in terms of the individual's interest in being left alone.[212] Subsequent cases have followed this formulation, although they often refer to the right to be left alone at one's home or office.[213]

The impact of a "right to be left alone" definition of privacy on the informational process is limited. It focuses solely on the act of intrusion and not on the acquisition of information. Therefore, if the intrusion is justified, the "right to be left alone" is not infringed, irrespective of the information that might be acquired. On the other hand, a right of informational privacy looks at the intrusion in terms of the information acquired. Questions such as the purpose of the acquisition of the information, the degree of confidentiality, the potential harm if the information is misused, will be relevant.

The Supreme Court of Canada in R v Dyment[214] has recognized that the right of privacy in section 8 includes inter alia a right to privacy in the informational context. La Forest J (Dickson CJC concurring) referred to Westins, Privacy and Freedom (1970),[215] that privacy was at the heart of liberty in a modern state and therefore was worthy of constitutional protection. La Forest J went on to adopt the conclusions of the "Report" "Privacy and Computers",[216] that there were three different aspects of privacy, territorial or spacial privacy, personal privacy and informational privacy. Informational privacy he held (again quoting from the same report):

> derives from the assumption that all information about a person is in a fundamental way his own to communicate or retain for himself as he sees fit.

It remains to be determined what impact the declaration of a right of informational privacy in section 8 will have in developing a more general right of privacy in section 7. In particular, it has been seen that section 8 was only a specific example of how section 7 might be infringed. (Reference re Section 94(2)of the Motor Vehicles Act)[217] In R v Racette,[218] the Saskatchewan Court of Appeal held that the right not to submit to unlawful search and seizure was but one aspect of the broad right to security of the person in section 7. If this is the case, then at least one aspect of section 7 includes a right to informational privacy, which has not yet been recognized by the courts. It is suggested that the decision in Dyment might hasten the recognition of a general right of privacy in section 7.

## (6) Conclusion

The influence of section 8 on the informational process is limited by a number of factors. First, section 8 deals only with one aspect of the informational process, namely the acquisition of information.[219] Secondly, it requires, as do all Charter provisions, that the applicant prove that his or her personal rights have been infringed.[220] Thirdly, the choice of relief availability to a litigant is limited. If the legislative scheme authorizing the search or seizure is valid, then the remedy most likely to be used under the Charter is the exclusion of evidence under Section 24(2).[221] This may not be appropriate in all cases. Even if it is relevant, its application in isolated instances might not have any general impact on informational standards. Fourthly, any right of privacy in section 8 may defer to other constitutionally protected rights.[222] Fifthly, as discussed, there must be some nexus between the intrusion and a search and seizure in section 8. Sixthly, even if section 8 is applicable to a particular situation, it will only require, at most, a warrant before the invasion of privacy is made.[223]

Nevertheless, despite these inherent limitations, section 8 has been interpreted broadly and affords considerable protection to the individual against the acquisition of information by government. Whereas section 8 might have been restricted to trespassory invasions of an individual's home or office, Southam and Dyment have provided broad protection to individuals against acquisition of information by government which infringes the individual's reasonable expectation of privacy, including reasonable expectation to informational privacy. It has also refused to restrict the application of section 8 by adopting a technical definition of search or seizure. Section 8 will thus effect not only the police and other law enforcement agencies in investigating criminal offences, but also government departments in an administrative context. The degree of section 8's application in the administrative field is still unclear. However, it is predicted that these departments will increasingly find that their commonly used methods of acquiring information, including, as discussed, demands for information, routine inspections and examination of files, the taking of samples and the seizing of papers, will have to conform to the requirements of section 8.[224] Changes in government methods of acquiring information will inevitably follow.

## PART 4 - SECTION 2(b)

### (1) Introduction

Section 2 Everyone has the following freedoms

(b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication.

Upon initial consideration, it is perhaps surprising to consider section 2(b) as providing protection to the individual against the abuses of informational technology, when there is so obvious a conflict between the rights of the individual to control the use of information concerning himself or herself, and the right of other parties to publish or disclose that same information.[225]

Section 2(b) does however, potentially provide protection to the individual against informational abuses in two areas. First, an individual may be deterred from exercising his freedom of expression because of the fear that expression will be recorded and the information acquired, at some subsequent time, will be used against him.[226] In such cases, it is said that the individual's freedom of expression has been chilled. If section 2(b) operates in this way, it is in effect providing protection to an aspect of an individual's privacy; his right to participate and express himself in society without unjustified government intrusion.[227]

Section 2(b) also potentially offers protection against the informational process if it is found that its protection extends to guarantee an individual's access to personal and public information. Such access rights are critical to the proper control of informational systems in that they allow the individual to determine the accuracy of personal information held by the government institution, and further facilitates personal discussion of policies.[228] Both access rights, therefore, provide a counter to government secrecy and anonymity.

## (2) Informational Practices Inhibiting Freedom of Expression

The proposition that freedom of expression may be chilled by surveillance depends on acceptance by courts of the invalidity of government action which has an indirect or psychological effect on the individual, thereby preventing the personal state necessary for that individual to exercise his or her freedom of expression. Canadian courts have not yet had to consider whether section 2(b) can be infringed by such indirect government action. In the U.S., however, the courts have held, in limited instances, that the recording of information may inhibit freedom of speech.[229]

The leading U.S. case is the decision of the Supreme Court in Laird v Tatum.[230] In that case the Army instituted widespread surveillance over individuals to secure information in relation to potential future civil disturbances. The applicants brought a class action claiming that the mere existence of the surveillance system of the Army imposed a chill on their first amendment (freedom of speech). The court dismissed the plaintiff's claim, holding that there was no justifiable dispute. The basis of this finding was that the applicants did not have standing to bring such an action as they had not sustained and were not in immediate danger of sustaining a direct injury as a result of government action. The mere fear that information might be used against them in the future was insufficient. Specific, present objective harm or the threat of specific future harm was required.

The decision in Laird v Tatum makes it clear that a broad based challenge to informational practices cannot be made through arguing chilling of freedom of speech. However, freedom of speech will be infringed where the applicant can prove more specific harm than the mere existence of information. This was implicitly recognized in Laird v Tatum, where the court held that there could be a:

> chilling effect of governmental regulations that falls short of a direct prohibition against the exercise of First Amendment rights.[231]

Cases involving loss of employment to the applicant[232] or denial of licensing[232a] are obvious situations where such direct harm to the individual may result, therefore providing the necessary standing.

There have been a number of cases subsequent to Laird v Tatum, where the courts have been able to find the necessary harm to the applicant, and thus distinguish Tatum on its facts. In Philadelphia Yearly Meeting of Religious Society of Friends,[233] it was held that surveillance, which was later shown on television, infringed the applicant's freedom of speech in that the harm of television disclosure "although not concrete was nonetheless strikingly apparent". In Berlin Democratic Club v Rimfield,[234] Tatum was distinguished on the ground that dissemination of the information would have resulted in possible termination of employment and destruction of reputation. Lastly, in White v Davis,[235] it was held that the standing rule in Tatum was based on a restrictive standing rule, which had no applicability to California where state legislation gave standing for class actions. These cases have led some observers[236] to suggest that there has been a retreat from the full rigours of Tatum. At the very least, it evidences an increased willingness to find direct harm to the applicant.

The preceding discussion of the U.S. position reveals two main issues for Canadian courts:

(i) Does section 2(b) include indirect infringement of freedom such as chill;

(ii) Will the same problems of standing limit the relevance, in the informational context, of this type of infringement of section 2(b).

Examining the first of these issues, the two most commonly suggested theories[237] for the constitutional protection of freedom of expression are either that it is necessary for the operation of democratic government or alternatively, that the autonomy of the individual requires the freedom to express and receive communications, free from interference by the State. In Canada, there is more judicial support for the democratic government theory. In Retail, Wholesale and Department Stores Union v Dolphin Delivery Ltd. the Supreme Court of Canada held that:

> freedom of expression is one of the fundamental concepts that has formed the basis for the historical development of the political, social and educational institutions of western society. Representative government as we know today, which is in great part the product of free expression and discussion of varying ideas, depends upon its maintenance and protection.[238]

This theory has been adopted by various courts[239] although in R v Zundel,[240] the Ontario Court of Appeal cited all the various theories, without deciding which one was appropriate.

Both the parliamentary an the autonomous theories of section 2(b), are sufficiently broad to encompass an indirect chill of section 2(b). Uninhibited political expression is obviously central to the democratic theory of freedom of expression; if individuals are prevented from expressing themselves, less information is available for discussion and democracy is harmed. Whether that prevention is direct or indirect is irrelevant; the same result is achieved.[241] At the minimum, the autonomy theory is concerned with expressions significant to the individual's development.[242] If expression is not imparted, the individual's development is impaired in that his views are not in the public domain and therefore not subject to public scrutiny. In addition, views received from other sources are restricted, therefore again limiting the individual's development.

Having suggested that the theory underlying section 2(b) allows for a chill infringement, we must next consider whether the standing limitation, as imposed in the U.S. cases, will also apply in Canadian courts. This will require proof pursuant to section 24(1) of the Charter, that the applicant's freedom of expression has been infringed. Often an applicant who brings a chill type action is not alleging that his or her personal freedom of expression has been impaired, but rather that government actions exercise a chill over the whole community. The interchange between counsel and the District Court Judge at D.C. level in Laird v Tatum[243] illustrates the point. The Justice asked counsel if the applicants were alleging that their personal freedom of expression had been infringed. The reply of counsel was no, but rather the action was being brought on behalf of the millions of citizens whose rights were so infringed.

It is submitted that in such a case, the applicant would also not have standing under section 24(1). In cases like Tatum, the applicant is, in reality, not so much arguing that his freedom of expression is infringed (which it often is not) but that his privacy has been infringed by the surveillance and maintenance of revealing information. It is therefore not surprising that attempts to invoke a less directly relevant section will run into procedural difficulty.

An impairment of an individual's freedom of expression under the Canadian Charter through the existence of a chill will, like the U.S., be limited to cases where the applicant can point to some personal deterrence in exercising his freedom of expression.

While section 24(1) does not expressly require the direct objective harm referred to in Tatum, it is suggested that on an evidentiary basis, a litigant under the Charter will have difficulty in proving that he has in fact been chilled, unless he can point to some objective reason for this discussion. A vague fear would not be sufficient to convince the courts that a legitimate chill had occurred. Cases involving dissemination or potential dissemination of information by the government will, therefore , be more likely to give the applicant standing under section 24(1), than cases where information is being merely maintained. Even if the applicant established a breach of section 24(1), he would, of course, be subject to the operation of section

1 of the Charter and the test laid down in R v Oakes.[244]

### (3) Freedom of Information and Section 2(b)

Freedom of information also coincides with informational technology concerns in the area of access to information. Freedom of expression requires as much information as possible being in the public domain. If access to information is restricted, then discussion and expression are consequentially curtailed. Access to information is also important to the informational process.[245] It is necessary that the individual be given the right to know what personal information is being collected, maintained and disseminated. Further, the public needs to be given access to information to monitor the activities of government.

The underlying basis for the protection of freedom of expression would suggest that access to public records is required. As Barron and Davies state:

> if the citizen is to perform his government function in democratic society, he must have the information necessary to properly evaluate governmental policy.[246]

The autonomy theory produces the same result. An autonomous individual must be capable of receiving information and evaluating that information to make his or her choice. If access to information is restricted, then the individual's autonomy is impaired by the withdrawal of certain information from the individual's perusal:[247]

> ... To the extent that the First Amendment is functionally designed to promote self realization, the gathering of knowledge and information constitutes a vital component of that right. Only if an individual is allowed to seek out the alternatives available to identify and evaluate the competing choice does the resulting expression views become more meaningful.[248]

The autonomy theory also justifies an individual's right of access to his or her personal records. Information about oneself is clearly critical to individual autonomy. However, it is difficult to use the democratic process theory as a justification for a right of access to personal information. The two concepts are simply not related in the majority of cases.

However, it is submitted for two reasons that this argument is unlikely to be accepted in practice. First, is the difficulty of establishing the categories of persons entitled to such access.[249] In the U.S. case of Zamel v Rusk,[250] the court held that the right to speak and publish does not carry with it the unrestricted right to gather information. The court went on to say that there were few restrictions on actions "which could not be clothed by ingenious argument in the garb of decreased data flow".[251] The second reason advanced is an unwillingness on the part of the courts to create an affirmative role for government institutions to secure freedom of expression;[252] instead the courts have only adopted the role of ensuring that government institutions do not directly curtail freedom of expression.[253]

For these reasons, the U.S. and Canadian courts have generally only considered access as a constitutionally protected right in cases involving newspaper access to courts. Therefore, in Re Southam Inc. v The Queen,[254] the court held that openness of the court was one of the hallmarks of a democratic society. One case that may have gone a little further was Re Ontario Public Service Employees Union and Attorney-General of Ontario,[255] where the court assumed, without expressly deciding, that the provision of money to a political party, while not directly expression, may buy or finance expression by others and therefore come within section 2(b).

It is suggested, that this case does not go against the two arguments stated above, which justify a refusal to include a general right of access within section 2(b). The group in Re Ontario Public Service Employees Union is clearly defined, and there is no affirmation action required on the part of the government institution.

It would, therefore, seem that, at present, a right of access is not included within section 2(b).

If, contrary to what we have said, section 2(b) may be breached by a denial of access to information, the government may, of course, have resort to section 1 of the

Charter to attempt to justify the infringement as a reasonable one in a democratic society. The test laid down in R v Oakes[256] will once again apply. However, certain issues peculiar to this area will arise. In particular, can bars to access information, erected under the Privacy Act and Access to Information Act, be justified under section 1 if they breach section 2(b).

Under section 18 of the Privacy Act, 22 databanks are exempt from the Act.[257] Most of these deal with law enforcement databanks. Clearly, section 18 satisfies the first part of the Oakes test of sufficiently important governmental objective. However, it is questionable whether the proportionality test is satisfied: is a total inapplicability of the Act to the exempted databanks impairing as little as possible upon the protected right? Further, is it necessary that there be a total exemption? The government would argue that only a relatively small number of banks have been exempted and would rely on cases such as Irwin v A.G. of Quebec,[258] where the Supreme Court of Canada held that because the impugned legislation only prohibited advertisements directed at persons under 13, it was a reasonable limit (that group only representing a small proportion of the total advertising audience). However, where there is a mechanism in the Privacy Act for the review of sensitive information,[259] one would question whether a complete exemption is necessary, and therefore justifiable, under section 1.

A second issue concerning section 1 and the Access to Information Act and the Privacy Act concerns the exclusion from the operation of the Acts cabinet records of the last twenty years.[260] As discussed previously,[261] cabinet records have been defined extremely broadly to include inter alia background reports, memorandum, records relating to preliminary deliberations and draft legislation. Again, one would argue that a complete prohibition of access to such materials goes far beyond what is necessary and is not the least intrusive measure that could be adopted. It seems almost unusually accepted that the cabinet records exemption as defined in the two Acts is undesirable and unnecessary in its breadth. Section 1 would not assist such unnecessary broadness. Any argument that the government might have that cabinet records are some unique category or documents, justifying exclusion from judicial scrutiny, is dispelled by the decision in Operation Dismantle v The Queen,[262] which allowed cabinet decisions to be reviewable.

In practical terms, a constitutionally enshrined right to access to information would expand access to information to the areas not covered at all by the Privacy Act or the Access to Information Act. (These acts only apply to those government departments listed in the first schdule of the Acts.)[263] It will also enable certain of the bars created by the Acts to be tested. The direct relevance of this to the informational process it two-fold; first, the individual is given the information necessary to challenge government actions, and in the public sphere, more information about the government process is being circulated.

### (4) Conclusion

The impact of section 2(b) on informational technology is clearly limited to particular areas where section 2(b), as well as protecting expression, also protects some aspect of an individual's privacy. Because the Charter has not yet produced any general theory of privacy, resort must be had to provisions such as section 2(b) which provide incidental protection to privacy. The difficulty in relying on such provisions, is that they are not designed to protect individuals against informational technology. When they attempt to do so, procedural problems such as standing may limit their effectiveness. Alternatively, the breadth of section 2(b), for example in the case of an individual's access to his own records, may be simply too narrow for informational concerns.

## FOOTNOTES - CHAPTER VI

1. Mackay "Fairness After the Charter: A Rose By Any Other Name" (1985) 10 Queens L.J. 263, 263. See also Dickson J. (as he then was) in Hunter v Southam (1984) 11 D.L.R. (4th) 641, 649

> a constitution, by contrast, is drafted with an eye to the future. Its function is to provide a framework for the legitimate exercise of government power and, when joined by a Bill or Charter of Rights, for the unremitting protection of individual rights and liberties.

2. S32. This Charter applies:

(a) to the Parliament and government of Canada in respect of all matters within the authority of Parliament including all matters relating to the Yukon Territory and Northwest Territories;

and

(b) to the legislature and government of each province in respect of all matters within the authority of the legislature of each province.

3. Mcllellan and Elman "To Whom does the Charter Apply? Some Recent Cases on Section 32" (1986) 24 Alta. L.R. 361, 370 citing Hogg, "Constitutional Law of Canada (2nd ed, 1985), 671.

4. Elliott "Interpreting the Charter: Use of the Earlier Version as an Aid" (1982) U.B.C.L.R. Charter Edition 11, 11. Tarnopolosky "A Comparison Between the Canadian Charter of Rights and Freedoms and the International Convention on Civil and Political Rights" (1982-3) 8-9 Queens L.J. 211, 214.

5. c.f. Spanish constitution which includes entrenched rights concerning data protection and secrecy - see Kirby "Human Rights - The Challenge of the New Technology" (1986) 60 A.L.J. 170, 171.

6. Kirby, Ibid, 170.

7. c.f. Universal Declaration of Human Rights, *G.A. Resolution 217 A(III), 10 Dec. 1948*, Art 12; International Covenant on Civil and Politicl Rights, *G.A. Resolution 2200 A(XII) 16 Dec 1968*, Art 17.

8. Tarnoplosky, supra n4 at 221.

9. Infra at p.104.

10. The leading U.S. case dealing with the chilling of freedom of association is *NAACP* v *Alabama* (1958) 357 U.S. 449; see generally Shattuck "*Rights of Privacy*" (1977), 47 ff.

11. Infra at Part IV.

12. See eg. Chalton & Gaskill *Encyclopaedia of Data Protection* (1988), 1002.

13. Supra at p.10 ff.

14. Ibid.

15. See *Reference re Prince Edward Island Lands Protection Act (1988)* 40 D.L.R. (4th) 1, 16 where quoting from *Reference re s94(2) of the Motor Vehicles Act* [1986] 1 W.W.R. 481, *R* v *Oakes* (1986) 26 D.L.R. (4th) 200 and *R* v *Big M Drug Mart* (1985) 18 D.L.R. (4th) 321, the court found that "the Supreme Court of Canada has recognized that one of the main purposes of the Charter is to champion human dignity and orth and sectin 7 has human emancipation as its objective, to enable an individual to realize his full worth within society".

16. (1984) 10 C.C.C. (3rd) 119, 114.

17. Colvin "Section Seven of the Canadian Charter of Rights and Freedoms" (1989) 68 *Can. B.R.* 560, 561.

18. (1988) 44 D.L.R. (4th) 385, 397. See also Re Kodellas and Saskatchewan Human Rights Commission (1987) 34 D.L.R. (4th) 30, 44 also made the same point.

18a. R v Big M Drug Mart supra n15; Reference re s94(2) Motor Vehicle Act supra n15; Re Budge and Workers' Compensation Board; City of Calgary (1988) 42 D.L.R. (4th) 649.

19. Reference s94(2) of the Motor Vehicles Act Ibid 491.

20. Ibid 493 approving Wilson J in Re Singh and the Minister of Employment and Immigration (1985) 17 D.L.R. (4th) 422, 458. See also Morgentaler v The Queen supra n18 at 398; also followed in Re Budge and Workers' Compensation Board; City of Calgary supra n18a at 665, R v Higgins (1988) 40 D.L.R. (4th) 600, 607; Borowski v A.G. of Canada (1987) 39 D.L.R. (4th) 731, 751-52, Reference re P.E.I. Lands Protection Act supra n15 at 16.

21. Ibid.

22. See the majority judgment of Lamer J in Reference re s94(2) of the Motor Vehicles Act supra n15 at 495. Wilson J dissented on this point (supra n15 at 512) but followed this approach in Morgentaler v The Queen, supra n18.

23. See Lamer J in Reference re s94(2) of the Motor Vehicles Act supra n15 at 495. Approved in Re Kodellas and Saskatchewan Human Rights Commission supra n18 at 44.

24. See Hogg "Constitutional Law of Canada" (2nd ed.), (1985) 744.

25. (1985) 19 C.C.C. (3rd) 137.

26. See the judgment of Nemitz C.J.B.C. citing from Warren J in Bolling v Sharpe (1954) 347 U.S. 497.

27. Supra n20 at 458.

28. (1972) 408 U.S. 564, 572.

30. Supra n20 at 486-7.

31. Ibid; see also Jones v The Queen (1987) 31 D.L.R. (4th) 569, 582 per Wilson J "liberty means freedom of the individual to develop and realize his potential to the full, to plan his own life to suit his own character, to make his own choices for good or ill, to be non-conformist, idiosyncratic and even eccentric - to be in today's parlance his own person and accountable as such".

32. Morgentaler v The Queen supra n20 at 486.

33. Ibid 488.

34. (1989) 53 D.L.R. (4th) 171, 192.

35. (1989) 57 D.L.R. (4th) 505, 512 ff.

36. Supra n20 at 397. "It is neither necessary nor wise in this appeal to explore the broader implicatinos of s7 as suggested by counsel. I prefer to rest my conclusions a narrower analysis. It is inappropriate to attempt an all encompassing explication of s7 so early in the history of Charter interpretation. The Court should be presented with a wide variety of claims and factual situations before articulating the full range of s7 rights."

37. See Augustine "Protection of the Right to Property Under the Canadian Charter of Rights and Freedoms" (1986) 18 Ottawa L.R. 56, 69 for initial doubts as to interpreting security of the person.

38. (1985) 18 C.C.C. (3rd) 137.

39. Supra n20, See esp. Wilson J at 459 f.

40. Ibid.

41. Ibid.

42. Supra n20 at 400 and 492; also adopted in *Re Kodellas and Saskatchewan Human Rights Commission* supra 18 at 45.

43. (1986) 29 D.L.R. (4th) 161, 218 "Additionally under s11(6), the security of the person is to be safeguarded as jealously as the liberty of the individual. In this context, the concept of security of the person is not restricted to physical integrity; rather it encompasses protection against overlong subjection to the vexations and vicissitudes of pending criminal investigation".

44. Ibid.

45. Supra n20 at 401.

46. Supra 15 at 495.

47. See MacKay supra n1 for a discussion, pre *Reference re s94(2) of the Motor Vehicles Act*, of the procedural/substantive argument. See also Hogg supra n24 at 746.

48. In *Reference re s94(2) of the Motor Vehicles Act*, supra n15, the court considered the actual use of the word "substantive" as misleading. Cf. *R v Robson* supra n38 where the court held that the principles of fundamental justice go to substantive and not procdure fairness. See also Mackinnon "Notes of Cases - Criminal Law - Felony Murder - S7 of the Charter of Rights and Freedoms - Criminal Law Reform - Vaillancourt v The Queen" (1988) 67 *Can B.R.* 350, 355.

49. *Reference re s94(2) of the Motor Vehicles Act* supra n15 at 495.

50. Supra n16 at 147.

51. Supra n20 at 401.

52. (1984) 11 C.R.R. 302, 310. The court expressly rejected a right of privacy argument made by counsel on the basis that such a right was rejected by the Joint Committee on the Repatriation of the Constitution Issue 46; 62. The court followed the unreported decision of *R* v *Yellowquill* (Man QB 1984).

53. (1987) 28 C.R.R. 63, 73 approving *R* v *Rowbotham* supra n52.

54. (1987) 31 D.L.R. (4th) 135, 137 holding that *Charboneau* was binding on it.

55. (1984) 10 C.C.C. (3rd) 119, 143.

56. (1965) 381 US 479.

57. Supra n20 at 508. Wilson J (p513) disagreed with this proportion and held that once the principles of fundamental justice were infringed, it was inconsistent to say that it could be justified under s1. However, in *Morgentaler* she followed the majority approach and applied s1 after finding a breach of the principles of jundamental justice. See McBean "The Implications of Entrenching Property Rights in S7 of the Charter of Rights" (1988) 26 *Alta*. L.R. 548, 561.

58. To use Wilson's J test in *Morgentaler*, supra at p

59. (1983) 32 C.R. (3rd) 117.

60. Writs of assistance authorize the hold to search for evidence of a particular kind of crime at any time and place as long as the holder of the writ occupies the office of police officer. Four federal statutes authorize the issuance of such a warrant, the Customs Act, the Excise Act, the Food

and Drugs Act and the Narcotic Control Act; see Hogg supra n24 at 753.

61. (1985) 18 C.R.R. 132.

62. Infra, Ch.VI, Part 3.

63. See Greenspan (ed) "Martin's Annual Criminal Code 1990; cc168-169.

64. See Reference re s94(2) of the Motor Vehicles Act supra 8 n15 at 495; see also R v Racette (1988) 48 D.L.R. (4th) 412.

65. Infra, Ch.VI, Part 3(3).

66. Supra at p.12.

67. Supra n20 at 399.

68. See Shattuck Rights of Privacy (1977) 157; He says that there will be an expungement of records in 3 situations: (i) when an arrest is not really an arrest; (ii) when arrest is for a minor offence - eg. disturbing the peace; and (iii) where arrest is unconstitutional.

69. (1974) 498 F. 2d 1017.

70. Infra at p.203.

71. See Shattuck supra n68 at 159 ff.

72. (1971) 400 U.S. 433; See Shattuck Ibid 154.

73. Supra n18 at 45 quoting McBain v Canadian Human Rights Commission (1984) 11 D.L.R. (4th) 203.

74. (1976) 424 US 693. For a general discussion see Shattuck supra n68 at 160.

75. (1976) 42 US 693, 712.

76. See Mackay supra n1 at 259.

77. s24(2) "Where in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute."

78. s52(1) "The Constitution of Canada is the supreme law of Canada, and any law that is inconsistent with the provisions of the Constitution is, to the extent of the inconsistency, of no force or effect."

79. See Mackay supra n1 at 283 for a discussion of the standard of proof required.

80. Supra at p.198.

81. (1973) F. 2d 180 cited in Shattuck supra n68 at 153.

82. (1959) 360 US 474.

83. Supra at p.189.

84. Lancaster "The End of Law" by O'Hagan (1987) 51 Sas LR 344, 345.

85. Supra at p.3.

86. Hunter "When Human Rights Become Wrongs" (1985) 23 U of Western Ontario L.R., 197, 198.

87. Supra at p.198.

88. See Shattuck supra n68 at 153.

89. (1973) 473 F. (2d) 180.

90. (1959) 360 US 474.

91. Supra n20 at 397 and 401.

92. Supra n56.

93. eg. Eisentadt v Baird (1972) 405 US 438; for a general discussion see Shattuck supra n68 at 105.

94. (1973) 410 US 113.

95. Ibid.

96. (1989) 57 U.S. Law Week 5023.

97. (1986) 478 US 186.

98. For a discussion of these cases see respectively Starke "The United States Supreme Court and the constitutionality of anti-abortion regulations" (1989) 10 A.L.J. 660 and Vieira "Hardwick and the Right of Privacy" (1988) 55 U of Chicago L.R. 1181.

99. Vieira Ibid.

100. Supra n52 at 310.

101. Supra n.53 at 74.

102. Elliott supra n4 at 14.

103. Hogg supra n24 at 748.

104. (1984) 11 D.L.R. (4th) 641.

105. See also R v Racette (1988) 48 D.L.R. (4th) 412, 446 where the court held that a breach of s8 was one example of how a right to security of the person was infringed.

106. Supra n15.

107. (1987) 26 D.L.R. (4th) 200. See also Reference re PEI Lands Protection Act supra n15 at 16 and R.L. Crain v Couture supra n16 at 143.

108. Supra n52 at 310.

109. See Eichbaum "Towards an Autonomy Based Theory of Constitutional Privacy: Beyond the Ideaology of Familial Privacy" (1979) Harvard C.R. C.L.L.R. 34.

110. (1958) E.T.S. No. 5; see Brownlie (ed.) Basic Documents in International Law (3rd ed., 1988), 320.*

111. Supra n7.

112. Supra n7.

113. (1987) 31 D.L.R. (4th) 569, 583. Wilson J. stated that the right to educate one's children is a facet of Art. 8(1) of the European Convention of the Protection of Human Rights and Freedoms.

114. Bender "The Canadian Charter of Rights and Freedoms and the United States' Bill of Rights: A Comparison" (1983) 28 McGill L.R. 811, 843 ff.

115. (1989) 55 D.L.R. (4th) 503, 513.

116. Ibid 514.

117. Ryan "Privacy, Orthodoxy and Democracy" (1973) 51 Can B.R. 84, 85-6.

118. Westin Privacy and Freedom (1967), 7.

119. Supra n16 at 151.

120. See Pe Potman and the Queen (1983) 2 C.C.C. (3rd) 383, 391-2 "Fundamental justice like the natural justice is a compendious expression intended to guarantee basic rights of citizens in a free and democratic society to a fair procedure. The principles or standards of fairness essential to the attainment of fundamental justice are in no sense static and will continue to evolve and develop in response to society's changing perception of what is arbitrary, unfair or unjust."

121. Supra at p.122.

122. R v Oakes has been approved numerous times in relation to s7; See eg. R v Grant (1987) 31 D.L.R. (4th) 127, 131; Jones v Queen (1987) 31 D.L.R. (4th) 569; Re Ginther and Saskatchewan Government Insurance (1988) D.L.R. (4th) 496; Morgentaler v The Queen (1988) 44 D.L.R. (4th) 385, 486.

123. (1986) 26 D.L.R. (4th) 200.

124. Supra n15 at 508; See also Re Singh and Minister of Employment and Immigratino, supra n20 at 469; R v City of Saulte Ste Marie (1978) 85 D.L.R. (3rd) 161, 171.

125. See Shattuck supra n68 at 182 citing Doe v Norton (1975) 422 US 391.

126. Ibid; Carriere "Euthanasia and Self-Determinism; Is There a Right to Die in Canada" (1987) 32 McGill L.J. 299, 312 where the author cites Professor Thompson that individuals forego their right of privacy when they are in receipt of

public funds.

127. (1987) 35 D.L.R. (4th) 433, 440.

128. (1987) 32 D.L.R. (4th) 39, 407 where the court held that even if the liberty to be protected by s7 is the parental right to be free from state intervention as suggested in Re T and the Catholic Children and Society of Toronto (1984) 46 O.R. (2nd) 347, that case recognizes that the application of s7 requires in some cases an obvious balancing of potential competing rights.

129. Supra n16 at 142.

130. Bender "Privacy" in Dorsen (ed.) Our Endangered Rights: ACLU Report on Civil Liberties Today (1984), 246 sees this as one of the major drawbacks of the 4th Amendment in the area of data protection.

131. (1984) 11 D.L.R. (4th) 641. For a general see Murray "The Reasonable Expectation of Privacy Test and the Scope of Protection against Unreasonable Search and Seizure Under Section 8 of the Charter of Rights and Freedoms" (1986) 18 Ottawa L.R. 25; Rosenberg "Case Comments: Unreasonable Search and Seizure: Hunter v Southam Inc." (1985) 19 U.B.C. L.R. 271; Finklestein "Constitutional Law - Search and Seizure After Southam" (1985) 63 Can. B.R. 178.

132. (1984) 11 D.L.R. (4th) 641, 652-3.

133. Dorsen, supra n130 at p246.

134. See Hunter v Southam Inc. (1984) 11 D.L.R. (4th) 641, 648-9; Collins v The Queen (1987) 38 D.L.R. (4th) 508, 521; Finklestein supra n131 at 188 ff says various Canadian statutes may prove unconstitutional in light of Southam.

135. (1967) 389 U.S. 347; For a discussion of U.S. 4th Amendment cases see McDonald "Legal Rights in the Canadian Charter of Rights and Freedoms" (1982),

45 ff.

136. Reid and Young "Administrative Search and Seizure under the Charter" (1985) 10 Queens L.J. 392, 394.

137. Ibid.

138. (1984) 11 C.R.R. 302.

139. (1985) 23 D.L.R. (4th) 532.

140. See MacLean "Video Surveillance and The Charter of Rights" (1987-88) 30 Criminal Law Quarterly 88, 97.

141. (1987) 33 D.L.R. (4th) 744, 752. In Thompson the court stated that in view of the concession made in Finlay, no argument was presented that the interception of electronic communication did not form part of s8.

142. See R v Playford (1988) 61 C.R. (3rd) 101, 143.

143. Ibid.

144. (1967) 38 U.S. 347, 351.

145. (1987) 34 C.C.C. (3rd) 51; For a general discussion of this case see MacLean supra n140; see also R v LeBeau; R v Lofthouse (1988) 41 C.C.C. (3rd) 163.

146. MacLean Ibid 100.

147. See Rosenberg supra n131 at 28 citing Oliver v U.S. (1983) 104 S.Ct. 1735; see also Bender supra n130 and 245 citing U.S. v White (1971) 101 U.S. 745; U.S. v N.Y. Telephone Co. (1977) 434 U.S. 159.

148. (1983) 460 U.S. 276; For a general discussion of

this case see Fishman "Electronic Tracking Devices Questions Still Unanswered" (1985) 34 Catholic University L.R. 277.

149. Ibid, 281.

150. Ibid; See also U.S. v Karo (1984) 104 S. Ct. R 329 discussed by Fishman supra n148.

151. (1989) 55 D.L.R. (4th) 503, 514.

152. See Bender supra n130 at 245.

153. (1970) U.S. 745.

154. Ibid 749 citing Hoffa v U.S. (1966) 385 U.S. 293.

155. Ibid.

156. Infra at p.230.

157. To use the language of Reid & Young supra n136 at 394.

158. For a general discussion of this issue see Finklestein supra n131 and Reid & Young Ibid.

159. Reid & Young Ibid 393.

160. eg. see Re College of Physicians & Surgeons of B.C. and Bishop (1989) 56 D.L.R. (4th) 164.

161. (1983) 1 D.L.R. (4th) 301.

162. Ibid 307.

163. (1984) 8 D.L.R. (4th) 696.

164. (1984) 8 D.L.R. (4th) 648.

165. (1987) 31 D.L.R. (4th) 449; on appeal (1987) 54 D.L.R. (4th) 705.

166. See also *Re International Escort Services Inc. and City of Vancouver* (1988) 55 D.L.R. (4th) 194 and *K Mart Canada Ltd.* v *Millmink Development Ltd.* (1987) 31 D.L.R. (4th) 135.

167. (1987) 34 D.L.R. (4th) 414.

168. See *R* v *McLinlay Transport Ltd.* (1987) 37 D.L.R. (4th) 454; on appeal (1988) 48 D.L.R. (4th) 765; also *Re New Brunswick Telephone Co. Ltd.* v *Kenney et al* (1989) 55 D.L.R. (4th) 711; *Re Gesham Produce Co. Ltd.* v *Motor Transport Bd* (1985) 22 D.L.R. (4th) 520.

169. Stone "The Inadequacy of Privacy" (1989) 34 *McGill L.J.* 685, 694.

170. [1986] 5 W.W.R. 667.

171. Ibid 673.

172. Ibid 674.

173. Finklestein supra n131 at 199.

174. Reid & Young supra n136 at 426 suggest that greater flexibility is required in relation to administrative searches and seizures.

175. Finklestein supra n131 at 202 suggests that Zeigler and Southam can only be rationalized if one takes the position, not addressed in Southam, that actual entry is a necessary element of privacy as that word is constitutionally interpreted.

176. (1989) 55 D.L.R. (4th) 503, 515.

177. Bender supra n130 at 247.

178. (1989) 55 D.L.R. (4th) 503.

179. Ibid 513.

180. Ibid.

181. See Hunter v Southam Inc. (1984) 11 D.L.R. (4th) 641, 654.

182. Ibid 653-657.

183. See Finklestein supra n131 at 194.

184. Re Ontario Chrysler (1977) Ltd. (1987) 39 D.L.R. (4th) 100.

185. This could be used to justify such cases as R v J.M.G. (1987) 33 D.L.R. (4th) 277 where the court held that the principal/student relationship was different from that of the policeman/citizen and therefore a warrantless search was justified by a principal who had to look after the integrity of students as a whole, including the offending student.

186. See R v Simmons (1989) 55 D.L.R. (4th) 673, 697.

187. (1984) 9 D.L.R. (4th) 542, 588. This point was made in Re College of Physicians & Surgeons of B.C. and Bishop (1989) 56 D.L.R. (4th) 164, 170.

188. (1985) 20 D.L.R. (4th) 156.

189. (1985) 24 C.C.C. (3rd) 78. Quesnel applied Belgoma and held that s8 was not infringed by an inspection of premises without warrant to ensure compliance with procedural quotas for regulation of farm products.

189a. (1987) 31 D.L.R. (4th) 210.

190. Ibid 249-50.

191. Applying the U.S. case of Donovan v Dewey (1981) 452 U.S. 594 which reached the same conclusion.

192. (1987) 33 D.L.R. (4th) 254.

193. The court expressly declined to follow the U.S. decision in Camar v Municipality of City and County of San Francisco (1967) 387 US 323, which required a warrant even for periodic inspections (unless in an emergency).

194. (1987) 33 D.L.R. (4th) 254, 264.

195. See R v Shepherd (1984) 11 C.C.C. (3rd) 276; Re Ontario Chrysler (1977) Ltd. (1987) 39 D.L.R. (4th), 100.

196. (1989) 55 D.L.R. (4th) 673.

197. Ibid 696.

198. Ibid.

199. (1987) 33 D.L.R. (4th) 254.

200. (1987) 37 D.L.R. (4th) 694.

201. Reid & Young supra n136 at 407-408; see also Stone supra n169 at 702.

202. Based on the Hunter v Southam criteria.

203. (1984) 11 D.L.R. (4th) 641, 656-7.

204. R.S.C. 1985, cC-46.

205. (1985) 23 D.L.R. (4th) 532.

206. Ibid 554.

206a. (1984) 11 D.L.R. (4th) 641, 660.

207. (1984) 34 C.R. (3rd) 337.

208. (1984) 8 D.L.R. (4th) 696.

209. eg. *R* v *Racette* (1988) 48 D.L.R. (4th) 412.

210. (1987) 34 D.L.R. (4th) 560, 563.

211. (1985) 23 D.L.R. (4th) 532, 559.

212. (1984) 11 D.L.R. (4th) 641, 652.

213. eg. *R* v *LaPlante* (1988) 48 D.L.R. (4th) 615 referred to the legitimate and reasonable expectation of privacy in one's home or office as a "prized right".

214. (1989) 55 D.L.R. (4th) 503.

215. Ibid 513.

216. Ibid 514. See "*Privacy and Computers, The Report of the Task Force est by the Dept. of Communications/Dept. of Justice*" (1972) 12-4.

217. [1986] 1 W.W.R. 481.

218. (1988) 48 D.L.R. (4th) 412, 446.

219. Bender supra n130 at 246.

220. Supra at p.202.

221. s24(2) requires exclusion of evidence if it is established that having regard to all the circumstances, the admission of it in proceedings would bring the administration of justice into disrepute: See Collins v The Queen (1987) 38 D.L.R. (4th) 508, 523.

222. As recognized: R v Dyment (1989) 55 D.L.R. (4th) 503, 515.

223. Bender supra n130 at 246.

224. Reid & Young supra 136 at 393.

225. See Shattuck "Rights of Privacy" (1977), 33.

226. Supra at p.24.

227. Shattuck supra n225 at 11. The same chill can occur in relation to freedom of association where an individual is chilled from exercising his right to associate with whom he chooses.

228. Kallner "Personal Data: The Open Access Approach" in O.E.C.D. "Policy Issues in Data Protection", Vol.10 Informatics Studies (1984), 59.

229. eg. See Menard v Mitchell (1971) 328 F. Supp. 718, 726 "Systematic recording and dissemination of information about individual citizens is a form of surveillance and control which may easily inhibit freedom of speech, to work and to move about.

230. (1972) 33 U.S. S. Ct. R 154.

231. Ibid 162.

232. eg. as in N.A.A.C.P. v Alabama (1958) 357 U.S. 449. See Shattuck supra n225 at 51.

232a. Shattuck Ibid citing Baird v State Bar of Arizona (1971) 401 US 1, Law Students Civil Rights Research Inc. v Wadmoimd (1971) 40 U.S. 154.

233. (1975) 519 F. 2d 1335; See Stickgold: Yesterday's Paronia is Today's Reality: Documentation of Police Surveillance of First Amendment Activity" (1978) 55 Journal of Urban Law 877 at 886, and Shattuck supra n225 at 83-4 for discussion of these cases.

234. (1976) 410 F. Supp. 144.

235. (1975) P. 2d 222.

236. See Stickgold supra n233 at 886; Shattuck supra n225 at 83.

237. For a good discussion of the various theoretical basis for protecting freedom of expression see Moon "The Scope of Freedom of Expression" (1985) 23 Osgoode Hall L.J. 331.

238. (1987) 33 D.L.R. (4th) 174.

239. See Re Fraser and Attorney-General of Nova Scotia (1987) 30 D.L.R. (4th) 340, 347; R v Kopayto (1988) 47 D.L.R. (4th) 213.

240. (1987) 35 D.L.R. (4th) 338. The Court said that differing theories had been expressed as to why freedom of expression should be guaranteed. These included the attainment of truth through the free exchange of idea; parliamentary democracy; self-fulfillment. The Court went on to say that in Retail, Wholesale and Department Stores, the Court applied the Parliamentary democracy theory.

241. Denvir "Justice Brennan, Justice Rehnquist and Free Speech" (1985) 80 N.W.U.L.R. 285, 304 said that the underlying basis of Justice Brennan's

theory of freedom of speech was based on his concern for the chilling effect of freedom of speech and its effect on a democracy.

242. Moon supra n237 at 333.

243. (1972) 33 U.S. S. Ct. R 154, 156.

244 (1986) 26 D.L.R. (4th) 200.

245. Kalner supra n228 at 59.

246. "Barron and Dienes" "Handbook of Free Speech and Free Press" in Magnet Constitutional Law of Canada (3rd ed. 1987), Vol. 2 993.

247. Ibid; see also Moon supra n237 at 333.

248. Barron and Dienes supra n246 at 370.

249. Ibid.

250. (1964) 381 U.S. 1.

251. Ibid 17; see Barron and Dienes supra n246 at 371.

252. Barron and Dienes Ibid.

253. Ibid.

254. (1983) 146 D.L.R. (3rd) 408, 414. See also Attorney-General of N.S. v MacIntyre (1982) 132 D.L.R. (3rd) 385, 400-401.

255. (1989) 52 D.L.R. (4th) 701.

256. (1986) 26 D.L.R. (4th) 200.

257. Privacy Act, 1980-81-82-83, c111, s18.

258. (1989) 58 D.L.R. (4th) 587 reversing decision of Quebec Court of Appeal in Irwin Toy Ltd. v Attorney-General of Quebec (1987) 32 D.L.R. (4th) 641.

259. Privacy Act, 1980-81-82-83, c111, s46, s51.

260. Privacy Act Ibid, s70. Access to Information Act 1980-81-82-83, c111, s69.

261. Supra at p.96.

262. (1985) 18 D.L.R. (4th) 481.

263. Privacy Act 1980-81-82-83, c111, s3 (definition of government institution); Access to Information Act 1980-81-82-83, c111 s3 (definition of government institution).

## CHAPTER VII - INTERNATIONAL PROTECTION

Since World War II, there has been vigorous growth in international protection of human rights. Such growth is evidenced primarily through the passing of the four major human rights instruments,[1] the Universal Declaration of Human Rights,[2] the International Covenant on Civil and Political Rights[3] (I.C.C.P.R.), the International Covenant on Economic, Social and Cultural Rights,[4] and in the European sphere, the European Convention on Human Rights.[5] Given the demonstrated inadequacy of domestic laws protecting privacy, resort to international law providing protection may be necessary.[6]

International protection against invasion of privacy caused by informational technology arises from a recognition in the Universal Declaration and the I.C.C.P.R. of a right to privacy:

> no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attack upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[7]

The relevance of these rights for Canadians will largely depend on whether or not a right of privacy can be implied in section 7 of the Charter. If it is, then the resort is not needed to the more explicit right in international law. International law has failed to go further in regulating informational technology - for example, there is no binding convention on data protection. The European Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data[8] illustrates the reluctance of the international community in this area[9] - there have been no ratifications of this convention.[10]

## PART 1. UNIVERSAL DECLARATION OF HUMAN RIGHTS

The Universal Declaration is a resolution of the United Nations' General Assembly, and as such will only have force if it can be said to have achieved the status of international customary law.[11] To constitute international customary law, there must be evidence of sufficient degree of practice of States in conformity with that law and a recognition by States that they consider themselves bound by the law.[12]

Though it is far from being undisputed, most writers agree that the Universal Declaration forms part of international customary law.[13] The decisions of the International Court of Justice frequently cite the Declaration and confirm its status.[14] In European, and increasingly in U.S. Courts,[15] the Declaration is cited. Canadian courts have been more cautious, and with the exception of Re Drummond Wren[16] there has been no decision importing, without reservation, the Declaration into

Canadian municipal law. Indeed, in Re Dixon and Manitoba Labour Board[17] and Re Noble and Wolf[18] the courts held the Declaration not to have the force of law in Canada.

Neither of these last mentioned decisions can be considered a satisfactory precedent. Re Noble and Wolf was decided just after the Declaration was made (1948), and when the degree of adherence by States was not as comprehensive as it is today. In Re Dixon the Court failed to give reasons as to why it came to its conclusion.

In further support of the Declaration achieving the status of customary law, is its universal acceptance by States in theory, (it was passed without dissent), the adoption of the Declaration in similar form in the National Constitutions of State,[19] and its recognition in other International Covenants.[20]

The arguments against the Declaration forming part of international customary law are two-fold. First, it is breached too frequently by States to achieve the necessary consensus. This argument seems to place too little emphasis on the recognition in theory of the Declaration by States, and the fact that the Declaration[21] as such is not suggestive of a particular result, but rather of factors to be considered. Secondly, one might look to the Declaration itself which says it is not to have the force of law[22] (it was envisaged that a binding convention would follow).[23] However, the very nature of customary law is that it is constantly changing. Therefore, while at the time it was made such an assertion would carry much weight, its relevance is reduced by the practice of States in the intervening years.

Assuming, therefore, that the Universal Declaration does form part of international customary law, the question arises to the incorporation of such law into the domestic law of Canada. There are two conflicting theories: the adoption theory asserts that international customary law is automatically part of domestic law;[24] the transformation theory requires a specific act of adoption (that is, legislation). It is generally accepted both by commentators[25] and by the courts[26] that the adoption theory is the law in Canada, though the position is not without debate, due primarily to the ambiguous statement of certain courts.[27]

The adoption theory is preferrable. First, it allows Canadian law to change as international customary law itself changes.[28] It appears illogical that international customary law is recognized because it reflects the adherence in practice by the States, yet the laws of the State do not themselves necessarily reflect the practice. Further, the transformation theory requires Parliament to ascertain what is international customary law, a task, it is submitted, that is better suited to the courts.[29]

This analysis suggests that the right of privacy in the Declaration may form part of the domestic law of Canada. Any action by a Canadian government, federal or provincial, infringing this right would be invalid. Although there has been no Canadian decision on this point, in the English case of Malone v Metropolitan Police Commissioner,[30] both the United Kingdom and European Courts recognized that the United Kingdom had violated the right of privacy guaranteed in Article 8 of the European Convention on Human Rights, by tapping telephones without a judicial warrant system.

There appears to be three major restrictions on the adoption of a right of privacy in this way. First, "privacy", as used in the Declaration, may be narrowly defined. Article 12 refers to interference with "privacy, family, home or correspondence". Cases to date have dealt with interference with some aspect of the individual's right to be left alone in his personal or intimate relationships, rather than a right of privacy in an informational context.[31]

A second, and more significant restriction, is the doctrine of Parliamentary Sovereignty[32] which ensures that Federal Legislature can override international customary law. The Charter does not override the Declaration - section 26 of the Charter provides that it does not abrogate other rights.[33] However, any other federal legislation can override international customary law and any right of privacy contained therein.

It is unclear whether a provincial legislation may also legislate in violation of international law. Various writers have suggested that they cannot,[34] relying on the decisions in Re Reference as to Powers to Lay Rates on Foreign Legations and High Commissioners' Residence[35] and Municipality of St. John et al v Fraser.[36] In these cases the Supreme Cout of Canada refused to permit taxation of a foreign government's residence by a municipal authority. There was no convention regulating these matters, and therefore it is argued that the basis of these decisions is that a provincial legislative cannot violate international customary law and therefore possibly embarrass the federal government.

It is submitted that such reasoning is unconvincing in that it fails to sufficiently recognize that the theory that the Crown is one and indivisible. Consequently, the provincial government is no "weaker" than the federal government but rather its competence extends into different areas.[37] Therefore, a better rationale of the cases is that the topic of legislation, taxation of the foreign government, was within the exclusion competence of the federal legislature. In other circumstances, a provincial government may be free to violate international customary law.

A third restraint on the effective use of the Declaration in domestic Canadian law lies in the nature of the Declaration. The Declaration arguably creates a set of principles rather than concrete rules - it exhorts member States to conform with the Declaration.[38]

## PART 2. INTERNATIONAL COVENANT ON CIVIL AND POLICITAL RIGHTS

The use of the International Covenant on Civil and Political Rights to incorporate a right of privacy into its domestic Canadian Law, is less likely. Although Canada ratified the Convention in 1976,[39] it has not legislated its enactment. It is an unequivocal constitutional rule that treaties do not form part of domestic Canadian law, unless incorporated by statute.[40]

It has been suggested that the Charter should be considered as implementing the Covenant.[41] The basis of this argument is that the legislation need not expressly refer to the treaty, which it is alleged to incorporate. Rather, the question of incorporation should be determined by an analysis of the language of the respective instrument.[42]

However, it is submitted that Canadian courts are most unlikely to hold that the Charter does enact the Covenant.[43] There are too many differences between the Charter and the Covenant.[44] For example, the Covenant contains an express right of privacy, right to a legal personality, right to be free from torture, right to marry etc.[45] There are no corresponding rights in the Charter.

The Charter was enacted at least in part because of the prevailing Canadian political situation,[46] hence the incorporation of dual language rights and native rights. The fulfillment of international obligations was not of primary concern.

The Covenant is thus likely to be used in a subsidiary way. First, because Canada has ratified the Covenant, an aggrieved party may petition the United Nations for relief.[47] Only in the Sandra Lovelace case[48] has a petition been made against Canada. The right to petition however, is available only when all domestic remedies are exhausted. The United Nation's Human Rights Committee has only the power to make recommendations, which do not bind the domestic court or parliament.[49] Thus, in the Lovelace case, the decision of the Supreme Court of Canada remains the law.[50]

The Covenant's practical application in Canada is therefore limited first to assisting the interpretation of domestic Statutes, especially the Charter. Obviously the similar language of the Convention and the Charter suggests the use of the Covenant as an aid in interpreting the new rights enunciated in the Charter. Secondly, there is a presumption that Canada does not intend to violate its international obligations.[51] Such a rule only applies where there is some ambiguity in the domestic statute.

## PART 3. CONCLUSION

The use of International Law to supplement the deficiencies of domestic Canadian law is a recourse to which adventurous counsel may have resort.[52] If the Canadian Legislature fails to specifically protect privacy (as we have demonstrated has been the case), privacy will only receive protection from rights derived from the Human Rights Statutes.[53] Whereas the right to privacy in the Charter is ambiguous, it is expressly enunciated in the Universal Declaration. However, the Declaration's status as international customary law is open to question. The courts are faced with the difficult task of interpreting customary law. One can therefore predict that the incorporation of a right to privacy by Canadian courts, in such a fashion, is likely to be cautious and restrictive. The Covenant must be expressly incorporated into domestic law.

Because of these drawbacks, one can expect that the right of privacy in international law will not provide a solution to the threat to our liberties caused by advances in informational technology.

## FOOTNOTES - CHAPTER VII

1. Brudner "The Domestic Enforcement of International Covenants on Human Rights: A Theoretical Framework" (1985) 35 U of Toronto L.J., 219.

2. U.N. General Assembly, 1948, Res. 217 (III) A; see Brownlie "Basic Documents in International Law" (3rd ed., 1983), 250.

3. U.N. General Assembly, 1966, Res. 2200 A [XXI]; see (1967) 61 A.J.I.L. 870; Brownlie supra n2 at 270.

4. U.N. General Assembly, 1966, Res. 2200 [XXI] Annex; see also 993 U.N.T.S. 3; Brownlie supra n2 at 258.

5. E.T.S. No.5; Brownlie supra n2 at 320.

6. Claydon "The Appliation of International Human Rights Law by Canadian Courts" (1981) 30 Buffalo L.R. 727, 750. "There exists great scope in integrating international human rights law with the domestic legislative system of Canada - such instances of its application have been few."

7. Universal Declaration of Human Rights, supra n2, Art. 12; I.C.C.P.R. supra n3, Art. 17.

8. Kirby "Human Rights - The Challenge of the New Technology" (1986) 60 A.L.J. 170, 177.

9. Ibid 193.

10. Ibid.

11. Woloshyn "To What Extent Can Canadian Courts Be Expected to Enforce International Human Rights Law in Civil Litigation" (1985) 50 Sas. L.R. 1, 3, cites Article 38 of the Statute of the International Court of Justice directing it to apply law derived from the following sources: (a)

International Treaties; (b) International Customary Law; (c) General principles of law recognized by civilized nations; (d) Judicial decisions.

12. Cohen and Bayefsky "The Canadian Charter of Rights and Freedoms and Public International Law" (1983) 61 Can. B.R. 265, 283.

13. Ibid citing the North Sea Continental Shelf Case (1963) 3 I.C.J. 3, where the International Court of Justice said, to constitute international customary law, you need (i) widespread and representative participation by States; (ii) State practice consistent with and generally recognizing the law.

14. See Humphrey "The Canadian Charter of Rights and Freedoms and International Law" (1985) 50 Sas. L.R. 13, 13. See also Claydon supra n6 at 733; Cohen & Bayefsky supra n12 at 271.

15. eg. See Cohen & Bayefsky Ibid citing Barcelona Tractor case [1970] I.C.J.R. 4, 32; Brudner supra n1 at 233 citing Rodriguez Fernadez v Wilkson (1982) 654 (2nd) Fd 138; Lareai v Anson (1981) 507 F. Supp. 1177, 1193.

16. [1945] 4 D.L.R. 674.

17. (1982) 127 D.L.R. (3rd) 252.

18. [1948] 4 D.L R. 133.

19. See Claydon supra n6 at 733.

20. eg. The Preamble to the International Covenant on Economic, Social and Cultural Rights (supra n4) states "considering the obligations of States under the Charter of the United Nations to Promote Universal Respect for the Observance of Human Rights and Freedoms".

21. Brudner supra n1 at 234 ff.

22. Woolshyn supra n11 at 7.

23. Cohen & Bayefsky supra n12 at 272.

24. Ibid; Claydon supra n6 at 729.

25. Ibid.

26. See *Gordon* v *R in Right of Canada* [1980] 5 W.W.R. 668, 671; *Re Royal Bank of Canada & Coriveau* (1981) 30 O.R. (2d) 653; *Chung Chi Cheung* [1939] A.C. 160 approved in *Reference as to Powers to Levy Rates on Foreign Legations and High Commissioner's Residence* [1943] S.C.r. 208.

27. See Duff CJ in *Reference as to Powers to Levy Rates on Foreign Legations and High Commissioner's Residence* (1943) S.C.R. 208, where he says that the law had been accepted and adopted by the Laws of England. The use of these words could be suggested as requiring some degree of transformation; see Claydon & Bayefsky supra n12 at 277.

28. Claydon & Bayefsky, Ibid 279.

29. Ibid.

30. [1971] ch.344.

31. eg. see Harris Cases and Materials on International Law (3rd ed., 1983), 552.

32. Woolshyn supra n11 at 9.

33. Cohen & Bayefsky supra n2 at 280.

34. See LaForest "May the Provinces Legislate in Violation of International Law" (1961) 39 *Can. B.R.* 78; see also Woloshyn supra n11.

35. [1943] S.C.R. 208, 214.

36. (1958) 13 D.L.R. (2nd) 77.

37. Claydon supra n6 at 730.

38. Brudner supra n1 at 226.

39. See Tarnoplosky "A Comparison Between the Canadian Charter of Rights and Freedoms and the International Covenant on Civil and Political Rights" (1982-4) 8-9 Queens L.J. 211, 211.

40. See Hayward "International Law and the Canadian Charter of Rights and Freedoms - Uses and Justifications" (1985) 23 U of Western Ontario 9, 9; Woloshyn supra n6 at 4; Cohen & Bayafsky supra n12 at 286 citing McDonald v Vapour (1976) 66 D.L.R. (3rd) 1, 3; Re Regina Palacses (1984) 7 D.L.R. (4th) 117.

41. Hayward Ibid.

42. Ibid.

43. eg. See Public Service Alliance of Canada v Queen (1985) 11 D.L.R. (4th) 337.

44. See Humphrey supra n14 at 15; Tarnoplosky supra n39.

45. Ibid.

46. Tarnoplosky supra n39 at 217.

47. See Zuisdwisk "The Right to Petition the United Nations Because of Alleged Violations of Human Rights" (1981) 59 Can. B.R. 103, 107.

48. Ibid 108. See (2nd) Report of the Human Rights Committee, 33 G.A.O.R. Supp. 40, para. 586, U.N. Doc A/33/40 (1978).

49. Ibid.

50. See Claydon supra n6.

51. Cohen & Bayafsky supra n12 at 267; Claydon supra n6 at 737 citing Capital Cities Communication v Canadian Radio and Television Commission (1977) 81 D.L.R. (3rd) 609; Re Mitchell and the Queen (1983) 42 O.R. (2nd) 481.

52. Woloshyn supra n11 at 88.

53. Kirby supra n9 at 179.

# CHAPTER VIII - CONCLUSION

The writer has suggested that informational technology, by giving government institutions the ability to collect, maintain and disseminate vast amounts of information, has impaired the civil liberties of individuals. It has done so directly, by giving power to government institutions to make decisions intimately affecting individuals, without reference to those individuals. It has also had an indirect effect on civil liberties, by preventing individuals from attaining the personal state necessary to exercise their liberties.

We have argued in this paper that in order to reverse this feeling of powerlessness and passivity in individuals and to encourage their exercise of civil liberties, the law must instill in the individual a belief that information is being handled fairly by government institutions and according to well articulated standards.

Our analysis of law relevant to the informational process has revealed it to be inadequate to achieve this objective. The law can be subjected to three general criticisms in relation to its operation to the informational process. It is inconsistent in its application, insufficiently sensitive to the privacy of individuals and lacks enforceability.

The lack of consistency is evident in the Privacy

Act, which constitutes the main legislative response to the informational process. This Act only applies to federal government institutions and not provincial government institutions (although this may be changed in the near future as a result of the review by a parliamentary committee, which has recommended extending the operation of the Act to provincial institutions).[1] Part VI of the Criminal Code, despite being headed "Invasion of Privacy", applies only to information gained by electronic interception of communications. Although section 8 of the Charter has been generously interpreted, it is restricted to acquisition of information. It does not, according to its present interpretation, apply to administrative demands for information, nor require administrative searches and seizures to be validated by warrant before being reasonable. The common law is even more erratic and its application to a particular situation will usually only occur where there is some blatant misdeed by government officials in the handling of information (eg. illegally obtained information or disclosure of false or confidential information).

The insensitivity to privacy concerns is reflected throughout the existing law. The Privacy Act does not contain a right of privacy. The Privacy Act and the Access to Information Act do give the individual a right of access to personal and public information. However, this is only one aspect of informational privacy and no right is given to individuals to exercise any control over information. The wide exceptions to access, including particularly the refusal of access to cabinet records of the past twenty years, restrict the right of access.[2]

Section 7 of the Charter has also not recognized a general right of privacy, though the Supreme Court of Canada in Morgentaler v The Queen[3] was careful not to foreclose the possibility of future recognition of that right. The decision in R v Dyment,[4] which held that section 8 of the Charter contained a right of privacy, including informational privacy, may be the impetus required for a recognition of a more general right within the ambit of section 7.

The common law also has not recognized a tort of privacy. Part VI of the Criminal Code is insensitive to privacy concerns by permitting, subject to obtaining a warrant, electronic surveillance in relation to the investigation of a wide range of offences. Lastly, although the provincial Privacy Acts do create a statutory tort of invasion of privacy, the wide exemptions as to what would otherwise constitute an invasion of privacy, effectively shield government institutions froum any action brought pursuant to the Act. The provincial Freedom of Information Acts (with the exception of Quebec and Ontario) only give rights of access to personal information and not other informational privacy rights.

The third general criticism of the existing law is its lack of enforceability. Again, the Privacy Act significantly fails in this regard. Although sections 4-8 of that Act do enact certain standards to be observed by government institutions when handling information, there is no mechanism in the Act for detecting or enforcing breaches of these standards. Under section 37 of the Act, enforcement of the standards lies with the Privacy Commissioner who may, from time to time, carry out investigations of databanks to ensure compliance with sections 4-8. He has no remedial powers, other than to report the matter to the head of the particular institution or to include it in his annual or special report.[5] The Ombudsman Act also suffers from a similar lack of powers of enforcement, although the Ombudsman's role is not specifically related to the informational process.

As a consequence of these general deficiencies in the existing law, the informational practices of government institutions are able to operate, for the most part, unchecked. Because of the subjective element involved in encouraging individuals to exercise their civil liberties, there is a need for the law to remedy these deficiencies before a widespread perception occurs throughout the community that information is being handling unfairly by government institutions. Unsupervised informational practices will contribute to such a perception.

It is suggested that both legislative and judicial reforms be implemented. These reforms, at least initially, can be made within the existing legal framework. The objectives of the proposed reform is two-fold; first, to create enforceable standards to be observed by government institutions when handling personal information; and secondly, to provide the individual with rights which can be used to challenge existing informational practices. The suggested reforms will involve both the Privacy Act and the Charter, in particular section 7. They are intended to allow a consistent approach to be adopted to the informational practices of government institutions.

In the legislative sphere, the main reform that needs to be implemented is a series of amendments to the Privacy Act. The Privacy Act is the only act, federal or provincial, which has the potential to apply to all aspects of the informational process. We have already suggested that a right of informational privacy ought to be included in the Act.[6] Such a right would not only increase the circumstances in which individuals were able to challenge informational practices of government, but would also influence the decisions of government officials when handling information.

As discussed previously,[7] an appropriate formulation of the right in the Privacy Act might be "Everyone in Canada has the right, subject to the provisions of this Act and subsection (2) hereof, to determine when, how and to what extent, personal information about themselves is held or communicated to others by governmental institutions". An exception to that right would read "Nothing in the preceding subsection shall effect the right of government institutions to hold or communicate information in accordance with the data protection principles." Further limited exceptions involving matters such as national security, international affairs, etc. may also be necessary. The enunciation of the data protection principles would also be set out in the Act. The individual would also be given suitable remedies for a breach of his right to privacy, including a right to claim damages.

A second group of amendments to the Privacy Act is suggested to facilitate greater use of the access rights. We have argued that access to information is an important aspect of informational privacy, and the amendments suggested are designed to make individuals aware of possible misuses of information and thereby exercise their access rights.[8] An individual should therefore be notified (subject to appropriate exceptions) whenever a government institution discloses information in accordance with section 8(2) of the Privacy Act, or wherever information is used by a government institution in relation to the employment of an individual, or the granting of a license or benefit to the individual. Sufficient notice would be given if the sources of the information diclosed or used by the government institution in reaching a decision, were revealed. It would also be desirable to restrict some of the present exceptions to access, most notably the cabinet records exemption.

The objective of the third group of amendments to the Privacy Act is to create a mechanism for the enforcement of informational standards. A right of informational privacy (with appropriate remedies) would only partly satisfy the need for enforceability. What is also required is for the Privacy Commissioner to assume greater powers of intervention and enforcement. A regular inspection by the Privacy Commissioner to ascertain compliance with informational standards is required. If these standards are in fact not being observed, the Privacy Commissioner might be able to appoint a delegate to oversee changes in the informational process of the institution, whereby compliance can be achieved. It is further suggested that each government institution appoint an informational officer, whose function is to ensure compliance with the enacted standards. At the end of the year, the officer would be required to submit a report to the Privacy Commissioner concerning the observance of these standards by the particular institution and detail what steps (if any) had been taken by the institution during the course of the year to ensure compliance. Such a report would assist the Privacy Commissioner in determining which institutions should be investigated more closely.

It is also necessary that the courts respond to the advances in informational technology, by recognizing various rights in individuals. To some extent, the courts have already demonstrated a willingness to do this. In section 8 of the Charter a right to privacy, including informational privacy, has been recognized. However, the interpretation of section 8 should be expanded to include, in appropriate circumstances, administrative demands for information as searches or seizures, and further to impose a warrant requirement on administrative searches and seizures. The impact of section 8 on administrative acquisition of information would then be greatly enchanged.

More importantly, a right of privacy should be recognized in section 7 of the Charter. As discussed previously, a right of privacy would make the loss of control of information a crucial issue in determining whether or not there had been an infringement of an individual's rights. If so, all government acts or legislation could be scrutinized to fairness, according to informational standards. At present, loss of information is only relevant if some other aspect of the individual's liberty or security of the person is infringed.

The precise formulation of a right of privacy in section 7 would of course be a matter of considerable debate but, for our purposes, we suggest that it must include a right to informational privacy, that is the right of the individual to determine when, how and to what extent personal information about themselves is held or communicated to others by government institutions.[9] Further, the use of data protection principles could apply to determine when the principles of fundamental justice had been infringed. This would ensure a consistent approach with the amendments that we have suggested to the Privacy Act.

If these legislative and judicial reforms are adopted, a more appropriate balance is struck, it is submitted, between the government role in carrying out its legitimate functions as efficiently as possible and the liberty of the individual.

## FOOTNOTES - CHAPTER VIII

1. Standing Committee on Justice, Open & Shut Enchancing the Right to Know and the Right to Privacy (Ottawa) Queen's Printer (1987).

2. Privacy Act, S.C. 1980-81-82-83, c111, s70. Access to Information Act, S.C. 1980-81-82-83, c111, s69.

3. (1988) 44 D.L.R. (4th) 385.

4. (1989) 55 D.L.R. (4th) 503.

5. Privacy Act, S.C. 1980-81-82-83, c111, s38-39.

6. Supra at p.116.

7. Supra at p.122.

8. Supra at p.104.

9. Westin, Privacy and Freedom (1967), 7.

# BIBLIOGRAPHY

## (I) BOOKS

Chalton S. and Gaskill S. (ed.), Data Protection Law (1988).

Chalton S. and Gaskill S. (ed.), Encyclopaedia of Data Protection Law (1988).

Cornish W.R., Intellectual Property (2nd ed., 1989).

Dorsen N. (ed.), Our Endangered Rights: ACLU Report on Civil Liberties Today (1984).

Dworkin R., Taking Rights Seriously (1977).

Gibson D. (ed.), Aspects of Privacy Law (1980).

Greenspan E.L., Martin's Annual Criminal Code 1990 (1990).

Hogg P.W., Constitutional Law of Canada (2nd ed., 1985).

Linden A.M., Canadian Tort Law (4th ed., 1988).

Magnet J.E., Constitutional Law of Canada (3rd ed., 1987).

Mann J.F., Computer Technology and the Law in Canada (1987).

Manning M., Protection of Privacy Act (1974).

Manning M., Wiretap Law in Canada (1978).

Miller A.R., The Assault on Privacy (1971).

Murray J.A. (ed.), *Informational Processing and the Right to Privacy: A Crossroads for North Americans* (1972).

Niblett B., *Data Protection Act 1984* (1984).

O'Brien D.M., *Privacy Law and Public Policy* (1979).

Rowe B.C. (ed.), *Privacy, Computers and You* (1972).

Rule J., McAdam D., Stearns L., and Uglow D. *The Politics of Privacy* (1980).

Shattuck J.H.F., *Rights of Privacy* (1977).

Sobels L.A. (ed.), *War on Privacy* (1976).

Turin R., *Privacy and Security in Personal Information* (1974).

Westin A.F., *Privacy and Freedom* (1967).

## (II) ARTICLES

Augustine P.W., "Protection of the Right to Property Under the Canadian Charter of Rights and Freedoms" (1986) 18 *Ottawa L.R.* 56.

Barron and Dienes, "Handbook of Free Speech and Free Press" in Magnet J.E. *Constitutional Law of Canada* (3rd ed., 1967), 370.

Benn A.W., "Technology and Society" in Rowe B. (ed.) *Privacy, Computers and You* (1972), 13.

Bloustein E.J. "Privacy as an Aspect of Human Dignity: An Answer to Dean

Prosser" (1965) 39 N.Y.U.L.R. 962.

Brudner A., "The Domestic Enforcement of International Covenants on Human Rights: A Theoretical Framework" (1985) 35 U. of T. L.J. 219.

Burns P., "Electronic Eavesdropping and the Federal Response: Cloning a Hybrid" (1975) 10 U.B.C.L.R. 36.

Burns P., "Privacy and the Common Law: A Tangled Skein Unravelling" in Gibson D. (ed.) Aspects of Privacy Law (1980), 21.

Burns P., "The Law and Privacy: The Canadian Experience" (1976) 54 Can. B.R. 1.

Carriere F., "Euthanasia and Self-Determinism: Is There a Right to Die in Canada" (1987) 32 McGill L.J. 299.

Claydon J., "The Application of International Human Rights Law by Canadian Courts" (1981) 30 Buffalo L.R. 727.

Cohen M. and Bayefsky A.F., "The Canadian Charter of Rights and Freedoms and Public International Law" (1983) 61 Can. B.R. 265.

Cohen S.A., "Invasion of Privacy: Police and Electronic Surveillance in Canada" (1982) 27 McGill L.J. 619.

Colvin E., "Section Seven of the Canadian Charter of Rights and Freedoms" (1989) 68 Can. B.R. 560.

Craig E.P., "Electronic Surveillance: Setting the Limits" (1975) 24 U.N.B.L.J. 29.

Davis D.R., "Police Surveillance of Political Dissidents" in Staff of Columbia H.R.L.R. (ed.) Surveillance, Dataveillance and Personal Freedoms Symposium (1973), 69.

Denvir J., "Justice Brennan, Justice Rehnquist and Free Speech" (1985) 80 N.W.U.L.R. 285.

Deutscher D., "The Protection of Privacy Act: Whose Privacy is it Protecting" in Gibson D. (ed.) Aspects of Privacy Law (1980), 141.

Donner F., "Electronic Surveillance: The National Security Game" (1978) 2 Civil Liberties R. 15.

Duncansson I. and Kerruish K., "The Reclamation of Civil Liberty" (1986) 6 Windsor Yr Book of Access to Justice 3.

Dworkin G., "The Common Law Protection of Privacy" (1976) 2 U. of Tas. L.R. 418.

Dworkin G., "Hard Cases" (1975) 88 Harvard L.R. 1057.

Eichbaum J., "Towards an Autonomy Based Theory of Constitutional Privacy: Beyond the Idealogy of Familial Privacy" (1979) Harvard C.R.C.L.L.R. 34.

Elliot R., "Interpreting the Charter: Use of the Earlier Versions as an Aid" (1982) U.B.C.L.R. (Charter ed.).

Faust S., "National Security Information Disclosure Under the FOIA: The Need for Effective Judicial Enforcement" (1984) 25 Boston College L.R. 611.

Fishman C.S., "Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo and the Questions Still Unanswered" (1985) 34 *Cath. University L.R.* 277.

Gavison R., "Privacy and the Limits of Law" (1980) 89 *Yale L.J.* 421.

Geddes E., "The Private Investigator and the Right to Privacy" (1989) 27 *Alta. L.R.* 256.

Gibson D., "Tort Law and the Charter of Rights" (1987) 16 *Man. L.R.* 1.

Hammond R.G., "Misappropriation of Commercial Information" (1986) 64 *Can. B.R.* 342.

Hayward M.A., "International Law and the Canadian Charter of Rights and Freedoms: Uses and Justifications" (1985) 23 *U of W. Ontario L.R.* 9.

Humphrey J., "The Canadian Charter of Rights and Freedoms and International Law" (1985) 50 *Sas. L.R.* 13.

Hunter I., "When Human Rights Becomes Wrongs" (1985) 23 *U of W. Ontario L.R.* 197.

Jacob J., "Some Legislative Proposals for the Proper Regulation of Databanks" in Rowe B.C. (ed.) *Privacy, Computers and You* (1972), 141.

Janisch H. and Irwin M., "Informational Technology and Public Policy: Regulatory Implications for Canada" (1982) 20 *Osgoode Hall L.J.* 610.

Kirby M., "Human Rights - The Challenge of the New Technology" (1986) 60 A.L.J. 170.

Lacovara P.A., "Presidential Power to Gather Intelligence: The Tension Between Article II and Amendment IV" (1976) 40 Law & Contemp. Problems 106.

LaForest G.V., "Fundamental Rights: The United Kingdom Isolated" (1984) Public Law 46.

Mackay W., "Fairness After the Charter: A Rose by Any Other Name" (1985) 10 Queens L.J. 263.

Mackinnon P., "Notes of Cases - Criminal Law - Felony Murder - Section 7 of the Charter of Rights and Freedoms - Criminal Law Reform - Vaillancourt v The Queen" (1988) 67 Can. B.R. 350.

Maclean S., "Video Surveillance and the Canadian Charter of Rights" (1987-88) 30 Crim. L.Q. 88.

Maloney, A., "The Ombudsman Idea" (1979) 13 U.B.C.L.R. 380.

Mann F.S., "Britain's Bill of Rights" (1978) 94 L.Q.R. 512.

Marshall, G., "The Right to Privacy: A Skeptical View" (1975) 21 McGill L.J. 242.

McBean J., "The Implications of Entrenching Property Rights in s7 of the Charter of Rights" (1988) 26 Alta. L.R. 548.

McDonald N., "Electronic Surveillance in Crime Detection: An Analysis of Canadian

Wiretapping Law" (1987) 10 Dal. H.H.L.J. 141.

McLaughlin B.M., "Education Rights and the Right to Privacy" (1981) 15 U.B.C.L.R. 176.

McIlellan A. and Elman B., "To Whom Does the Charter Apply? Some Recent Cases on Section 32" (1986) 24 Alta. L.R. 361.

Miller A.R., "Computers, Databanks and Individual Privacy: An Overview" in Staff of Columbia H.R. L.R. (ed.) Surveillance, Dataveillance and Personal Freedoms Symposium (1973), 11.

Moon R., "The Scope of Freedom of Expression" (1985) 23 Osgoode Hall L.J. 331.

Nesson C.R., "Aspects of the Executives Power Over National Security Matters: Secrecy Classifications and Foreign Intelligence Wiretaps" (1973) 49 Indiana L.J. 399.

Niblett G.B.F., "Computers and Privacy" in Rowe B.C. (ed.) Privacy, Computers and You (1972) 17.

Onyshko T., "Access to Personal Information: British and Canadian Legislative Approaches" (1989) 18 Man. L.J. 213.

Osborne P.H., "The Privacy Acts of British Columbia, Manitoba and Saskatchewan" in Gibson D: Aspects of Privacy Law (1980) 73.

Parker R.B., "A Definition of Privacy" (1974) 27 Rutgers L.J. 275.

Prosger, "Privacy" (1960) 48 *California L.R.* 353.

Rankin M., "Privacy and Technology: A Canadian Perspective" (1984) 22 *Alta. L.R.* 323.

Rankin M., "The New Access to Information and Privacy Act: A Critical Annotation" (1983) 15 *Ottawa L.R.* 1.

Reid A.D. and Young A.H., "Administrative Search and Seizure Under the Charter" (1985) 10 *Queens L.J.* 392.

Rosenberg M., "Case Comments - Unreasonable Search and Seizure: Hunter v Southam Inc." (1985) 19 *U.B.C.L.R.* 271.

Ryan E.F., "Privacy, Orthodoxy and Democracy" (1983) 51 *Can. B.R.* 84.

Sawer G., "The Ombudsman Comes to Alberta" (1968) 6 *Alta. L.R.* 95.

Schafer A., "Privacy: A Philosophical Overview".

Selmer K., "Standards for Information Handling and Control Procedures" in *O.E.C.D. Policy Issues in Data Protection and Privacy* (1974) *Informatics Studies 10*.

Sharp J.M., "Privacy in Canada" in Rowe B.C. *Privacy, Computers and You* (1972) 63.

Sharp J.M., "Some Proposals for Legislation in Canada" in Rowe B.C. *Privacy, Computers and You* (1972), 129.

Starke J.G., "The United States Supreme Court and the Constitutionality of Anti-Abortion Regulations" (1989) 63 *A.L.J.* 660.

Stone R., "The Inadequacy of Privacy" (1989) 34 *McGill L.J.* 685.

Tarnoplosky W.S., "A Comparison Between the Canadian Charter of Rights and Freedoms and the International Covention on Civil and Political Rights" (1982-83) *Queens L.J.* 211.

Viera N., "Hardwick and the Right of Privacy" (1988) 55 *U of Chigago L.R.* 1181.

Washburn P., "Electronic Journalism, Computers and Privacy" (1981) 3 *Computer L.J.* 189.

Westin A.F., "Some Forecasts Based on U.S. Experience" in Rowe B.C. (ed.) *Privacy, Computers and You* (1972), 53.

Williams J.S., "Invasion of Privacy" (1973) 11 *Alta. L.R.* 1.

Woloshyn D.F., "To What Extent Can Canadian Courts be Expected to Enforce International Human Rights Laws in Civil Litigation" (1985) 50 *Sas. L.R.* 1.

Zuijdwijk T.J.M., "The Right to Petition the United Nations Because of Alleged Violations of Human Rights" (1981) 59 *Can. B.R.* 103.